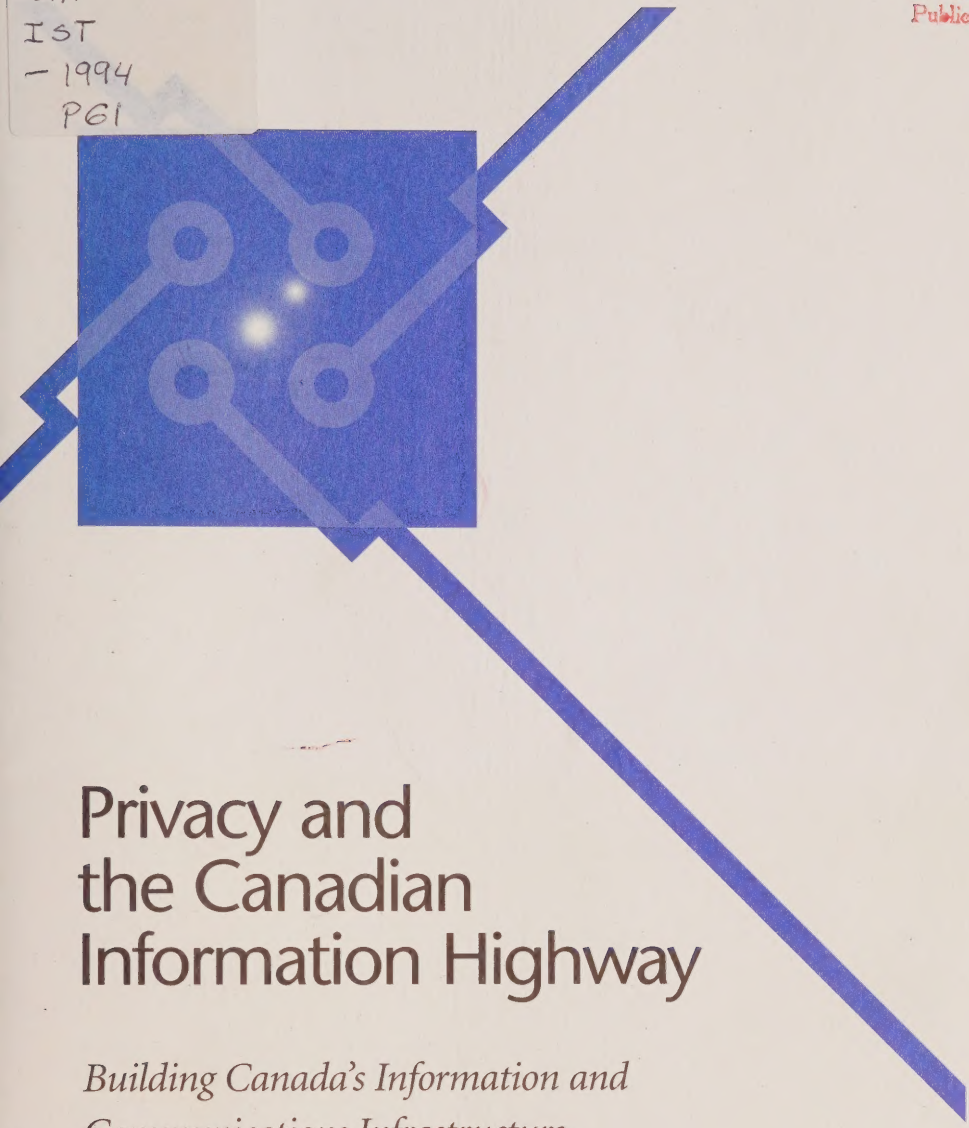
PRIVACY AND THE CANADIAN INFORMATION HIGHWAY: BUILDING CANADA'S INFORMATION AND COMMUNICATIONS INFRASTRUCTURE

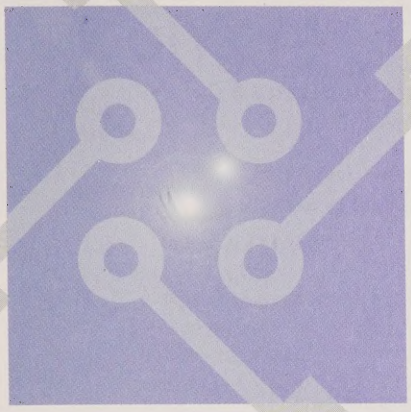


Privacy and the Canadian Information Highway

Building Canada's Information and Communications Infrastructure

Industry Canada Industrie Canada

Canada



Privacy and the Canadian Information Highway

Communications Development and Planning Branch
Spectrum, Information Technologies
and Telecommunications Sector
Industry Canada
October 1994

Privacy and the Canadian Information Highway and many other Industry Canada documents are available electronically on the Internet computer network at council@istc.ca.

Anyone with the ability to use Anonymous file transfer (FTP), Gopher or the World Wide Web can access these documents. Below are the Internet addresses:

Anonymous file transfer (FTP)
debra.dgbt.doc.ca/pub/isc

Gopher
debra.dgbt.doc.ca port 70/Industry Canada Documents

World Wide Web
http:/debra.dgbt.doc.ca/isc/isc.html

Additional print copies of this discussion paper are available from:

Distribution Services
Industry Canada
Room 208D, East Tower
235 Queen Street
OTTAWA, Ont
K1A 0H5
Tel.: (613) 954-5716
Fax: (613) 954-6436

A campanion document, *The Canadian Information Highway: Building Canada's Information and Communications Infrastructure,* is also available from this address.

For information about the contents of this discussion paper and the consultation process, contact:

Information Highway Advisory Council Secretariat
Room 640, Journal Tower North
300 Slater Street
OTTAWA, Ont.
K1A 0C8
Tel.: (613) 990-4268
Fax: (613) 941-1164

Cat. No. C2-229/1-1994
ISBN 0-662-61370-8
SIT PU 0025-94-03

Contents

Preface

The information highway of the future might be more accurately described as the advanced information and communications infrastructure that is essential for Canada's emerging information economy. Building on existing and planned communications networks, this infrastructure will become a "network of networks," linking Canadian homes, businesses, governments and institutions to a wide range of interactive services, from entertainment, educational and cultural products to social services, data banks, computers and electronic commerce as well as banking and business services.

Industry Minister John Manley in March 1994 created a national Information Highway Advisory Council to assist the federal government in developing and implementing a strategy for Canada's information highway. It is the council's responsibility to provide the necessary advice and guidance to government on the variety of issues raised in the government's discussion paper *The Canadian Information Highway: Building Canada's Information and Communications Infrastructure* (Ottawa: Minister of Supply and Services Canada, 1994), prepared by Industry Canada. Within this framework, the council will be examining how an advanced information infrastructure will improve the growth and competitiveness of Canadian businesses; how to ensure universal, affordable access to essential services for all Canadians; how to develop an appropriate balance between competition and regulation; and how to promote the development and distribution of Canadian culture and content.

Five working groups have been established by the advisory council to cover the following broad areas of interest: Access and Social Impact; Canadian Content and Culture; Competitiveness and Job Creation; Learning and Training; and R&D, Applications and Market Development. The working groups and the council meet on a regular basis and are engaged in a variety of activities to explore the issues, consult with the public and make recommendations to the federal government.

To seek the public's views and to raise the level of debate on privacy issues, Industry Canada is releasing the discussion paper *Privacy and the Canadian Information Highway* in cooperation with the advisory council. It is the first of several discussion documents to be released by Industry Canada on social, economic and technology policy issues. Written submissions and/or comments are invited from all interested parties on the various options and approaches presented or on any portion of this discussion paper.

Submissions should be addressed to:

Parke Davis, Director General
Information Highway Advisory
Council Secretariat
Room 640, Journal Tower North
300 Slater Street
OTTAWA, Ont.
K1A 0C8

All submissions must be received on or before December 23, 1994 (see *Canada Gazette,* Part I).

Two weeks after the closing date for comments, all submissions will be made available for viewing by the public, during normal business hours, at:

Industry Canada Library
2nd Floor, Journal Tower South
365 Laurier Avenue West
OTTAWA, Ont.
K1A 0C8

and at the regional offices of Industry Canada in Halifax, Montreal, Toronto, Edmonton and Vancouver for a period of one year.

Introduction

Businesses, public institutions and governments gather, store, transmit and exchange vast amounts of personal and business-related information both in paper format and electronically. The shift to computer-mediated interaction and the interconnection of networks will increase the amount of personal and transactional information that can be assembled into comprehensive profiles of individuals. In many cases, these records can be sent across national borders, sold or reused, or integrated with other data bases, for purposes unrelated to those for which the information was originally collected, without the consent of or compensation to the individual from whom the information was obtained. There is no question that the ability to access, repackage and resell information can benefit individuals and firms, and create new employment opportunities. On the other hand, it raises concerns among the general public, the business community and government alike about privacy protection and the security of sensitive information.

Public surveys of Canadians have consistently revealed a remarkably high level of concern over the issue of privacy. The 1992 Canadian Privacy Survey by Ekos Research Associates Inc. found that 92 percent of the 3 000 Canadians interviewed believed privacy to be an important issue, and that 60 percent believed they have less personal privacy now than a decade ago. Respondents also indicated they would be more at ease with others using their personal information if they had control over this information, knew their privacy rights were protected and knew government exercised some form of oversight or monitoring of these activities. A 1994 Gallup Canada survey for Andersen Consulting revealed that over 80 percent of the Canadians polled expressed concern about the personal information about them that might be collected by companies through the information highway. These studies suggest a pervasive belief that personal privacy is under siege from a range of technological, commercial and social threats and that something must be done about it. What is the role that government, businesses and individuals should play? What concerns must be addressed? What options are available?

Under the Canadian Constitution, the protection of privacy is a shared jurisdictional responsibility of the federal and provincial governments. In fact, Canadians are only partially protected by a combination of federal and provincial legislation, and voluntary codes set by government and the business community. The adequacy of Canada's current legislative framework for privacy protection is reviewed briefly in this paper, as are recent efforts, both federal and provincial, to broaden and enhance this framework to meet new privacy concerns.

In the "network of networks" world that is now emerging, Canada forms a part of the international "information grid" or "global village." As a sovereign nation, Canada has international commitments to a variety of treaties and conventions; as a trading nation and as a leader in communications technology and services, Canada has an interest in how other nations solve the privacy challenges facing us now. This paper also outlines Canada's participation in international organizations concerned with privacy protection and the efforts of some of our trading partners in this area. Finally, several approaches are proposed to strengthen personal privacy and data protection in Canada.

What Is Privacy?

Privacy is usually defined in two ways: the right to be left alone, free from intrusion or interruption, and the right to exercise control over one's personal information.

We Canadians value our right to live in peace, undisturbed by others. It is the right to solitude, to anonymity, to share our time with those we choose, and to define our own space and boundaries. This concept of privacy encompasses a broad range of issues that go beyond the acquisition and dissemination of personal information. While the *Canadian Charter of Rights and Freedoms* does not contain a specific right to privacy, it does guarantee an individual in his or her dealings with government the right to life, liberty and security of person, and the right to be secure from unreasonable search and seizure. Many privacy experts, however, would question the effectiveness of the protection available under the Charter.

Personal data protection has been defined as the claim of individuals to determine when, how and to what extent information about them is communicated to others. Data protection is an aspect of privacy protection that involves control over the collection, storage, accuracy, use and dissemination of personal information.

The high degree of mobility of modern Canadian lifestyles brings us into contact with a great many people who may not know us personally, except through various types of information we provide about ourselves. In travelling, shopping, obtaining services, driving our vehicles, and communicating from different locations, there is a need for us to provide secure identification of who we are and what we are entitled to receive. Service providers of all kinds require and ask for detailed information that will verify our identity and confirm our ability to pay. At the same time, these details and the data trails left by electronic transactions can be used to predict future marketing opportunities and thus increase the incentive to store this personal information in data bases. The exchange and marketing of personal information is flourishing, and it is increasingly taking place across national borders. As a result, data protection is becoming the most critical component of privacy protection.

Privacy Issues for the Information Highway

Transactional Data and Personal Profiling

Transactional data gathering will become much easier in a computer-mediated and networked world. The great strides in computing capacity, the linking of so many businesses by electronic payment systems, and the meshing of sales and ordering data bases have revolutionized the relationship between consumers and the producers of goods and services. With "just-in-time" supply management, producers manufacture and ship goods to warehouses and suppliers in direct response to the data transmitted from the point-of-sale terminals of their clients. Wholesalers and retailers increasingly are plugging into the chain. The linking of an individual to a particular purchase is merely one more segment of the chain, which facilitates direct marketing and market analysis. Most people may be aware that a credit card company could be selling their transactional data to vendors of products, but they might consider this a reasonable cost of doing business with a huge and reliable credit company, and one outweighed by the benefits. In the new networked environment, every business — large or small, reliable or not — will have the capacity to generate information files on its customers or to purchase customer data bases from other sources. What is the appropriate balance between the social and commercial benefits of such advanced technologies and the risks they bring to individual privacy? What controls or safeguards should be placed on the use and reuse of this information?

The information highway holds enormous potential to easily compile profiles of individuals' needs, lifestyle habits or purchase choices. This could have negative consequences if such profiles are used to deny opportunities to people without their knowledge. Data base storage and information cross-matching can be used to make decisions about individuals, affecting the terms and conditions of access to a variety of products, services and employment opportunities. This capability could further stigmatize the vulnerable — such as those who are ill, elderly or unemployed, or those who are seeking welfare, health care or citizenship — limiting their chances and curbing the gains we have made in equity and human rights in our society. In a highly competitive job market, where thousands of people send in résumés for

even modest jobs, what kinds of data base screening are we prepared to accept? How can unsuccessful job candidates ensure that they were not passed over because of erroneous information that appears on their records? Should organizations be required to notify individuals of their information holdings and provide no- or low-cost access to these files for verification or correction? Should there be time limits on the storage of information?

Provision of new services such as video on demand, and electronic magazines and catalogue services on the highway will permit the collection of an ever wider range of information regarding one's interests and choice of entertainment and reading material. Is some form of regulation needed to limit storage, access and use of such detailed data? Is it safe to permit such systems to gather information about our habits, even for benign purposes? How can individual privacy rights be protected during the different steps of the information collection, storage and exchange processes? Should informed consent be required for the different information activities and transactions an organization can undertake using personal information?

Transactional Security and Individual Identification

While encryption or encoding can secure the content of the electronic message, verifying the identities of the sender and the receiver is an equally critical element of privacy. This is especially true for financial and commercial information exchanges or for sending sensitive information. Increasingly, ordinary consumer transactions are not conducted in person, but through a variety of means, such as telephones, faxes or catalogue orders. Present methods of authentication and payment arrangements require various kinds of personal information that are not easily known by others, ranging from one's credit card number to the maiden name of one's mother. The extension of these commercial transactions at the consumer level to the terminal in the home poses new challenges. How can one verify a person's identity and/or credit worthiness for electronic orders or requests for delivery of medical records? Will present identification procedures continue to be adequate on the information highway? Would other methods, such as digital signatures, prove more secure?

Identity Cards and Single Identifier Numbers

Another aspect of the privacy debate is the issue of identity cards. New "smart card" technologies afford organizations the means of going beyond the limited information currently stored in magnetic strips to the enormous storage capacity of embedded chips. Detailed information or even pictures of the individual could be encoded on the card, or the data linked to a biometric identifier such as a thumbprint or retinal scan. With the current rates of fraud in card-based authorization systems — be they credit, phone or medical benefits cards — there is growing pressure to move to a more reliable system of identification. Privacy advocates, however, fear the potential of such cards to facilitate unacceptable levels of data matching, or the creation of a society in which it will be mandatory to carry identification documents on one's person at all times. In the face of strong public support for decreasing fraud in our social programs,

where is the line between responsible administration of programs and services, and unacceptable loss of individual liberties and privacy? A single numerical identifier increases the capability to amass and cross-match personal information. Should there be limits on such identifiers?

In the field of health information, privacy is a sensitive issue. Doctors, clinics and hospitals, insurers and governments, epidemiologists and researchers are motivated by differing interests with respect to health records, and may want access to lifelong data for legitimate purposes. But individuals, also legitimately, fear the abuse of this information by benefit providers or employers. In a Quebec trial use of a smart card for medical services, the information stored on the card was sequestered into four quadrants, with each service provider (such as a pharmacy) having access only to the information required. This solves one privacy problem because all players in the medical system are unable to access the complete range of patient data. However, the more fundamental issue of maintaining cradle-to-grave records through advances in technology remains a problem where privacy protection is not comprehensive.

Monitoring and Surveillance

Lifestyles, working patterns and business transactions will be transformed as computing and network power enter every home and business. While each information technology has different capabilities, they all contribute to an unprecedented capacity for surveillance of every man, woman and child, whether as customer, student, employee, patient, taxpayer or recipient of government services.

One of the most widely used applications on computer networks is electronic mail. The efficiency and convenience of this new information system have brought instant popularity in both commercial and social settings. Should employee e-mail be treated as a private letter, or as company property and therefore available to be read by a system operator or by a supervisor? Should these systems be designed to allow for easy encryption or encoding of the messages, to protect against casual forwarding and broadcasting of sensitive messages? Just as conventions and etiquette have been developed for the handling of personal and business correspondence over the centuries, should these norms be adapted to our new electronic environment?

Teleworking or working at home also brings a risk of increased surveillance. Managers may want to measure the productivity of employees who work at home by counting keystrokes, timing phone calls or wiring video cameras to the network. These techniques are already in use in some specialized areas of the work force. What limits, if any, need to be imposed on such monitoring? Is government regulation required, or will encouraging good behaviour and fair contracting practices suffice?

The information highway promises to support banking, teleworking, utility and appliance management, and other monitoring activities in the home. This raises serious questions not only about security of data on the network, but also about security in the home, whereby an intruder could enter and force the homeowner to withdraw money or to

credit another account through the home computer system. Home surveillance and protection systems offer security from burglary and fire, but how intimate should such systems be? Must there be a video data stream of every doorway and accessible window in our house sent to a security company or the police department? What controls should be put in place for the collection, use, availability and possible resale of information gathered about our use of different services in the home?

Another category of personal information is provided through satellite technology for global mobile telephone coverage. There will soon be available a unique individual telephone number that travels with each person, from the workplace to the home, the cottage, friends' apartments or businesses and other trips. Local cellular systems and other new personal communications services will have a similar capacity to track phones, using conventional radio and microwave technology. The gains in convenience are obvious, but the catch is that the computer must know exactly where each person is at all times. Privacy advocates want to know who will control the information about our whereabouts, how long it will be kept, and how far this "electronic leash" will extend. How should the different interests of employees and employers be balanced in this and similar forms of monitoring?

Intrusion

Citizens may also want to be protected from unwanted communications as a result of purchasing goods on the electronic highway. Disturbances or intrusions by telemarketers or targeted advertising mail is a privacy nuisance that concerns many Canadians. There is already "junk" fax, with solicitations over our fax machines for everything from coffee service to holiday trips. Should controls target marketing schemes that result from separate or related purchases — for instance, junk e-mail that follows a purchase of a Caribbean holiday with offers for a next trip? If so, how? What rules should govern the collection and use of information about what people buy or other personal information transactions? How should these rules be balanced with the opportunity to be made aware of goods or services that people might want and need?

What Privacy Protection Now Exists in Canada?

Over the past 20 years, the history of data protection legislation in the developed world has reflected the effort to balance what democratic countries perceive as the fundamental right of privacy and the need for government and business to obtain personal information that allows individuals to participate in a complex global society (see Annex A). Codes of fair information practices began to emerge, which limited the collection of information and established the right of the individual to access his or her own data, challenge its accuracy and correct any inaccuracies. During the 1970s, the Organisation for Economic Co-operation and Development (OECD) recognized the need to address the issue of personal privacy in the context of the growing transborder flow of information. Member countries, including Canada, started work on a set of guidelines. In 1981, the OECD released its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (see Annex B). Canada and other member countries adopted the Guidelines and indicated that they would be addressing privacy issues, either by passing legislation that incorporated the principles or by putting in place voluntary systems that would give force to them.

Protection in the Public Sector

Canada employs a mixture of legislation and voluntary codes to protect privacy. Data protection legislation protects personal information held by governments at the federal level and at some provincial and municipal levels. Based on the OECD Guidelines, the federal *Privacy Act* of 1982 protects information held by the federal government. The Office of the Privacy Commissioner was created to monitor the federal government's collection, use and disclosure of its clients' and employees' personal information, and its handling of individual requests to see personal records. In their annual reports to Parliament, Privacy Commissioners have not limited their comments to data protection within the federal government, but have reported on privacy trends across Canadian society. The cause of privacy protection has benefited greatly from these activities.

Some of the provinces have followed suit and have passed comprehensive legislation, starting with Quebec in 1982, Ontario in 1987, Saskatchewan in 1991, British Columbia in 1992 and Alberta in 1994. Nova Scotia introduced a privacy bill for the provincial public

sector in 1993. The powers of the various provincial commissioners or ombudsmen vary. For example, the British Columbia Commissioner can make binding orders, while the Ontario Commissioner makes recommendations. Only the Quebec Commissioner has jurisdiction over the private sector, with the power to impose fines for non-compliance of up to $20 000.

In Quebec, the issue of privacy has been addressed differently, partly because the Quebec *Civil Code* contains a specific and detailed right of privacy that covers private as well as public information holdings. Quebec has gone further than any other province by passing legislation that protects all personal information held by both the public and the private sectors. This legislation came into force in January 1994. It is one of the first data protection laws of its kind outside Europe, and has already had the effect of encouraging national operations to harmonize to the standard of data protection that must be met in Quebec.

Protection in the Private Sector

Apart from this effort in Quebec, the rapidly expanding use and management of personal information in the private sector is virtually unregulated in Canada, although there have been attempts in specific sectors to voluntarily set and implement fair information or privacy codes. These codes attempt to define boundaries and establish guidelines for personal privacy protection in order to achieve a balance between social and economic benefits, and an individual's right to control over his or her personal information.

The Canadian Direct Marketing Association, for example, has a voluntary code that offers consumers a chance to "opt out" or refuse to let their data be passed on or sold to other companies, and enjoins its members to make their best efforts to help consumers find out where erroneous information may have crept into their files.

The banking sector has had a privacy code since 1991, although the code and its implementation have fallen short of the expectations of privacy advocates, largely on the issues of client access to personal information and the amount of information required for granting credit. In public hearings in 1993, the Canadian Senate explored draft regulations that would address banking privacy concerns, should the Minister of Finance decide in the future that there is a need to regulate in this area. There has been no formal call, however, to move on this proposal.

The telecommunications sector has a mixture of a voluntary approach and regulation. The introduction of caller identification service, which displays the telephone number of the person calling, was criticized by a broad coalition of concerned citizens — from women's shelters to seniors' groups — for its inherent infringement on privacy. Telephone companies were eventually required by the Canadian Radio-television and Telecommunications Commission (CRTC) to offer free per-call blocking, and line blocking for those with particular needs. Around the same time, the privacy of cellular and mobile phones received widespread media attention after the private conversations of public figures were recorded using electronic scanners. In response to these

and other concerns, such as the proliferation of telemarketing and junk fax, the federal government announced a set of Telecommunications Privacy Principles (see Annex C) in December 1992. These principles were designed to encourage awareness of privacy concerns within the industry and to promote a self-regulatory approach. They reinforced the rights of individuals to control their personal information and to be made aware of the privacy implications of new communications and information technology products and services. Although the Telecommunications Privacy Protection Agency, which was proposed to oversee the implementation of these principles, has never materialized into an active force, the principles have influenced the development of voluntary codes within the telecommunications sector.

The new *Telecommunications Act,* which came into effect in October 1993, provides the CRTC with enhanced powers to protect the privacy of individuals and to regulate unsolicited communications. The government also introduced amendments to the *Criminal Code* and the *Radiocommunication Act,* which came into effect in August 1993, forbidding the divulgence of intercepted radio-based telephone communications.

In addition to these sector-specific initiatives, Canada is experimenting with a more inclusive national model code. In the fall of 1990, the Canadian Standards Association (CSA) initiated the development of a national privacy standard that could be applied across all sectors and all provinces. Several federal departments, key private sector players and various consumer representatives are participating in this initiative, and a draft code is expected to be available for public comment late in 1994. With a standards-based approach to data protection, privacy could be addressed during the development of new information and communications technologies, and could be promoted with our trading partners internationally. A national standard for data protection developed in Canada could be included as an element in the International Organization for Standardization's quality management standards (ISO 9000 series), increasing the likelihood that large corporations would treat the management of personal data in the same way they do security, clean room facility management and other quality control mechanisms.

How Have Other Countries Protected Privacy?

The European approach to privacy favours omnibus data protection regulations that apply to both the public and private sectors, and are overseen by independent data commissioners. Countries whose histories have made them sensitive to data protection issues, such as Germany, France, Austria and Sweden, passed laws in the 1970s and, by the end of that decade, there was sufficient imbalance of protection in Europe that the Council of Europe began to discuss a Convention that would bind member countries to producing similar legislation. The OECD developed its Guidelines in 1981 in order to provide the same kind of harmonization among its member states, fearing that the disparity in protection of privacy rights would cause countries with data protection to block the flows of data to those without it. By the end of the 1980s, many European countries had still failed to produce data protection legislation, even though they were obliged by Convention 108 of the Council of Europe. The Commission of the European Community, concerned that data commissioners might block data transfers between countries and thus hinder the development of a single European common market, decided to act.

In 1990, the Commission of the European Community released two draft data protection directives, which, if passed by the European Parliament, will have the force of law. The first was a general directive applying to all personal data, computerized or in manual files, which banned data flows to countries without adequate protection. The second was a tightly modelled directive on privacy in telecommunications, which dictated the precise response member countries and trading partners should take to the intrusions posed by caller identification, cellular and speaker phones, and call detail recording. Response to this initiative was swift, with many businesses and member countries opposed to various aspects of the directive. In 1992, the main directive reappeared with greatly reduced extraterritoriality, and a later version is expected to be passed by the end of 1994.

In contrast, the United States has tended to rely on voluntary codes of practice and sectoral legislation. In 1970, the U.S. passed the first *Fair Credit Reporting Act*, recognizing that the detailed profiling necessary for credit activities must be balanced by opportunities for consumers to examine

their files and correct errors. The federal *Privacy Act* was passed in 1974 to protect the privacy of individuals with respect to information contained in federal government records that was likely to be released under the new *Freedom of Information Act* (FOIA). However, the emphasis was clearly on the FOIA, and there was no independent oversight of the *Privacy Act.* In response to scandals in the credit business, the United States is revising its fair credit reporting legislation.

The United States is also taking a fresh look at privacy in the context of its National Information Infrastructure (NII) initiative, which is similar to Canada's efforts to seek advice on what the future information highway should be. It has struck a task force to look solely at privacy issues. The Working Group on Privacy of the NII Task Force has tabled privacy principles for comment, but the oversight mechanisms are as yet unspecified. The National Telecommunications and Information Agency, the arm of the Commerce Department responsible for policy advice on the NII, has issued a call for comment on the implications for privacy of new telecommunications services, with a discussion paper exploring some of the issues in transaction-generated information.

Possible Approaches for Canada

Most Canadians doubt their ability to protect their privacy, and see the role of protection as a government responsibility or a joint government/business partnership. Undoubtedly, the development of the information highway will continue to raise these issues and the demand for action.

Possible approaches to privacy protection include legislation, the advancement of a national voluntary privacy standard, the promotion of privacy protective technologies such as encryption and smart cards, and consumer education. Canada may need all of these approaches.

Legislation and Regulation

Protection of the enormous information holdings of governments, including medical, welfare, tax, immigration and police records, exists at the federal level and in the provinces of Quebec, Ontario, Saskatchewan, Alberta and British Columbia. The quality of coverage varies from jurisdiction to jurisdiction and, when information travels, it is not always clear which law applies. Reflecting this environment in its 1993–94 annual report, the Office of the Privacy Commissioner described Canada's privacy protection as a patchwork of public and private initiatives that address privacy in a piecemeal fashion. The commissioner called for "national privacy legislation to establish the principles and framework" for both business and government. There is no doubt that both provincial commissioners and governments have recognized these problems too, and it may be time to initiate a dialogue to work toward solutions.

Although federal legislation may well be desirable to provide uniform protection and rights across Canada, the division of authority between federal and provincial jurisdictions appears to preclude this from happening. The federal government has the power to regulate industries such as telecommunications, transportation carriers and banks. The provinces, however, have responsibility for privacy protection in areas such as individual transactions between consumers and the retail industry. By amending existing sectoral legislation, the federal government could create privacy protection requirements in each sector it regulates. Another possible approach would be to extend the federal *Privacy Act* to all sectors of the marketplace within federal jurisdiction. Since this might further exacerbate disparities between regulated and non-regulated entities, it would make sense for jurisdictions to work together toward a common set of rules that could be applied in all sectors.

Federal legislation would respond to the expressed desire of Canadians for a government oversight role in consumer protection. It could also serve to initiate a dialogue for improved privacy protection at the provincial and territorial level. A complementary federal and provincial framework could address such shared concerns as the potential for interprovincial trade barriers caused by differing privacy protection requirements and practices among provinces and territories. It would have to address the need for a level playing field between competing businesses and for consumers coast to coast. The private sector currently faces different regulatory regimes. For example, the privacy protection clauses of the *Telecommunications Act* apply to federally regulated carriers, but not to telecommunications resellers and information service providers. The cost of meeting differing standards is passed on to consumers in the prices of goods and services.

Many segments of the population would favour a legislative approach. The 1992 Canadian Privacy Survey found that a clear majority of Canadians favoured government legislation or a government/private sector partnership to develop privacy protection guidelines for the private sector. A 1992 Equifax Canada study of Consumers and Privacy in the Information Age found that 84 percent of the insurance, financial and credit bureau executives surveyed believed that federal legislation is required to set rules for the collection and circulation of consumer information, thereby avoiding a patchwork of disparate provincial regimes. While this appears to go against today's trend toward a deregulatory environment and reduction of government, it may in fact recognize that harmonized basic rules for data protection are good for business and may be possible without excessive bureaucracy. Setting ground rules enables all players to compete fairly, and establishes consumer confidence.

Voluntary Codes and Standards

Voluntary codes have been the preferred approach of Canadian business and industry associations. This approach allows for flexibility in application, so that different industries can tailor their data protection schemes to the needs of their customers, the regulatory environment in which they operate and the demands of the marketplace.

There is no need for voluntary codes to be any less stringent than those enforced by law, but it is this very matter of enforceability that is giving consumer advocates grounds for concern. Who is ultimately accountable? To whom does an aggrieved consumer go for redress? As the value of personal information increases with the growth of the information economy, how can voluntary codes unsanctioned by law ensure its protection? Past experience with voluntary codes has not been encouraging because they frequently do not meet the 1981 OECD Guidelines. As a result, they are considered by most privacy experts as inadequate to cope with the privacy threats of the 1990s.

The CSA's project to develop a national privacy standard extends the voluntary code approach. By setting out the basic principles that must be addressed in a code, the standard strengthens the often weak and ambiguous language used in codes. Oversight in the form of auditing and certification by a standards

body, such as the Quality Management Institute, a division of the CSA, could provide a level of protection similar to that in a legislated regime. Successful privacy protection by means of the proposed CSA voluntary standard, however, will be difficult if it is not adopted fully and implemented broadly by industry associations and companies.

Contractual approaches also have been suggested, whereby consumers would agree to the use of their data for specific purposes, perhaps in return for discounts or fees. Care must be taken that such a market-driven approach does not result in privacy for only the rich. At present, few individuals understand the market value of their personal information or know how to protect it. In addition, contracts that limit or waive fundamental privacy values have the potential to become an industry practice in the absence of clearly defined privacy rights.

Technological Solutions

Another approach to privacy protection is to use technology to safeguard personal data. Traditionally, technology has been exploited to increase the amount of information gathered, and hence has been feared rather than welcomed by privacy activists. But technology itself is neutral, and can be used to enhance privacy as well as threaten it. Technologies can be designed so that the "default setting" is on zero information collection. Telephone systems can be designed to "forget" the last few digits of a telephone number after placing a call, in order to protect privacy in personal billing statements. Electronic mail systems can be developed that provide ephemeral messages for personal use, a sort of electronic disappearing ink. Should the design for the information highway explicitly enhance the ability of the individual to control his or her personal and transactional information?

An important yet underexplored territory is encryption or encoding. Strong encryption is now available and can be incorporated into software, embedded as chips in equipment such as telephone sets or palm-sized computers, or used in smart cards. Smart cards, through the use of public key encryption, can provide fraud-proof guarantees of identity or credentials, and yet allow the holder to be completely anonymous. The same technology can be used to provide reliable but virtually untraceable electronic cash — a far safer method for the consumer than releasing a charge card number over the information highway.

Technologies brought to market can have profound effects on the rights of consumers, but how can consumers affect the technology development process? Should there be public hearings, such as the CRTC has for telecommunications services when a new technology is brought to market? Should the privacy implications of all new information systems and standards be explored in public fora? Is it a responsibility of government, or should it be up to the marketplace to determine what levels of privacy protection will be offered? Should privacy be an optional extra, for which only some Canadians can afford to pay, or should privacy be cost-neutral and considered an essential part of service offerings?

Consumer Education

There is a fundamental need to educate businesses about the need for more enlightened approaches to the handling of personal data, and to raise the awareness of consumers about how to protect themselves. Consumers need information and education about their rights, about the value of their personal information, about the risks to their privacy that new technologies can bring, and about what they can do to retain privacy. Although most Canadians see the role of protecting privacy as a government responsibility or perhaps a partnership of government and business, they also feel that the individual has a strong role to play in solving privacy problems. What should be the relative balance of responsibilities?

Public Comment

The intent of this paper is to contribute to the debate on the social and economic impact of the information highway, not to offer definitive solutions. Comments from individuals, organizations and institutions in both the private and public sectors are welcome. Written submissions and/or comments on the approaches to privacy protection are invited on the following questions, or on any portion of this discussion paper. They should be sent to the address mentioned in the Preface.

- What principles should form the basis of effective privacy protection?
- Does government need to introduce stronger measures to protect the privacy and security of information? How can each of the four approaches described above be used effectively?
- Is a national level of privacy protection needed, or can adequate privacy protection on the information highway be provided through provincial or sectoral legislation?
- In which circumstances might voluntary privacy guidelines developed by businesses be appropriate?
- Should the information highway be designed to provide high levels of privacy protection, or will this slow the pace and raise the cost of innovation?
- How can Canadians become better involved in the design process for potentially privacy-threatening technologies and services?
- How can Canadians become better informed about the value of their personal information and the need for controlling its use? What role should businesses and governments play in educating the public?

Annexes

A — Chronology of Background Events

The issue of privacy in an information-based economy arose globally in the 1970s. In Canada, the former Department of Communications joined with the Department of Justice in forming the Task Force on Privacy and Computers, which issued a report titled *Privacy and Computers* (Ottawa: Information Canada, 1972) and several studies. At the OECD, privacy was addressed as an issue of transborder data flows. Member countries realized that they had a common interest in protecting privacy and individual liberties, and in reconciling the fundamental but competing values of privacy and the free flow of information. It was recognized that transborder flows of personal data contribute to economic and social development, and that restrictions on these flows could interfere with the operations of multinational enterprises and cause serious disruptions in important economic sectors such as banking, insurance and travel. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were promulgated. At about the same time, the Council of Europe passed a similar document, Convention 108, to which European countries varied greatly in their legislative responses. It was the sluggishness on the part of member states to take action that prompted the European Community to introduce much stiffer Community directives with the force of law.

Key events and players are listed below in chronological order:

1969 OECD recognizes privacy implications of transborder data flow; Group of Experts struck in 1978

1970 U.S. *Fair Credit Reporting Act*

1972 Report of the joint Justice–Communications task force on privacy and computers

1977 Privacy Commissioner established under *Canadian Human Rights Act*

1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

1981 Interdepartmental Task Force on Transborder Data Flows struck in Canada

1982 Council of Europe passes Convention 108 on data protection; Canada passes *Privacy Act* for federally held records

1984 Canada signs OECD Guidelines; Department of Justice responsible for urging compliance of industry

1987 Report of Standing Committee on Justice reviewing *Privacy Act* implementation criticizes lack of compliance with OECD Guidelines in private sector and government inertia

1990 European Community tables draft directives on data protection and data protection in telecommunications; U.S. and international players mount vigorous lobby to water down transborder data flows and trade-restrictive aspects of directive

1991 OECD revisits data protection; European Community seeks to protect its privacy directives in the General Agreement on Tariffs and Trade; key federal departments back CSA's bid to develop a model OECD-based code of practice, along with industry and consumer groups

1992 Department of Communications tables Telecommunications Privacy Principles and drafts legislation on cellular privacy

1993 Federal government passes new *Telecommunications Act,* which came into effect October 25, 1993, giving CRTC a specific mandate with respect to the protection of privacy in telecommunications and substantial powers to exercise this mandate; Quebec passes Bill 68, law on protection of personal information in the private sector, which came into effect January 1, 1994

B — The OECD Guidelines and the Draft CSA Privacy Standard

Drafted at the end of the 1970s and adopted as a recommendation of the Council of the OECD in September 1980, the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data provided a sound basis for fair information practices at the time, and constituted a remarkable document for a group of countries largely without data protection laws. Nevertheless, the Guidelines may require some further specifications in the context of the technologies of the 21st century. The main concepts are as follows:

- Eight basic principles of national application are set out in Part Two of the Guidelines, covering data Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation and Accountability.
- Four principles of international application covering Free Flow and Legitimate Restrictions are set out in Part Three of the Guidelines.

When the CSA went about drafting its model privacy code, it used the OECD Guidelines as a starting point, interpreting them afresh in the Canadian context of 1991. It is important to evaluate the CSA standard in its entirety, since the commentary on the principles is important to the understanding of each principle. However, because the draft is not yet available for public discussion, its 10 principles are listed below only briefly, with a note where there is deviation from the OECD Guidelines. Public comment on the final draft will be invited in the fall of 1994.

1. Accountability (seen to be so fundamental that it must be the first principle)
2. Identifying purposes
3. Consent (new)
4. Limiting collection
5. Limiting use, disclosure, retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance (new; gives individual the right to challenge an organization's compliance with any of the principles, not just the accuracy of the individual's data)

C — *Telecommunications Privacy Principles*

- Canadians value their privacy. Personal privacy considerations must be addressed explicitly in the provision, use and regulation of telecommunications services.
- Canadians need to know the implications of the use of telecommunications services for their personal privacy. All providers of telecommunications services and government have a responsibility to communicate this information in an understandable and accessible form.
- When telecommunications services that compromise personal privacy are introduced, appropriate measures must be taken to maintain the consumers' privacy at no extra cost unless there are compelling reasons for not doing so.
- It is fundamental to privacy that there be limits to the collection, use and disclosure of personal information obtained by service providers and generated by telecommunications networks. Except where clearly in the public interest, or as authorized by law, such information should be collected, used and disclosed only with the express and informed consent of the persons involved.
- Fundamental to privacy is the right to be left alone. A balance should exist between the legitimate use of unsolicited telecommunications and their potential for intrusion into personal privacy. All parties have a responsibility to establish ground rules and methods of redress so that Canadians are able to protect themselves from unwanted and intrusive telecommunications.
- Privacy expectations of Canadians may change over time. Methods of protecting telecommunications privacy must be reviewed from time to time to meet these changing expectations and to respond to changing technologies and services.

C — *Principes de protection de la vie privée dans les télécommunications*

- Les Canadiens accordent une grande importance à leur vie privée. Les facteurs relatifs aux renseignements personnels doivent être exposés explicitement dans les documents sur la prestation, l'utilisation et la réglementation des services de télécommunications.
- Les Canadiens doivent connaître les répercussions de l'utilisation des services de télécommunications sur leur vie privée. Il incombe à tous les fournisseurs de services de télécommunications ainsi qu'à l'administration publique de communiquer ces renseignements, de manière compréhensible et accessible.
- Lorsqu'on introduit des services de télécommunications qui font intrusion dans la vie privée, il faut prendre des mesures appropriées pour protéger la vie privée du consommateur sans frais supplémentaires, sauf dans des cas exceptionnels.
- Il est indispensable pour la vie privée qu'il y ait des limites à la collecte, à l'utilisation et à la divulgation de renseignements personnels obtenus par les fournisseurs de services et de produits par les réseaux de télécommunications. Sauf dans les cas qui sont clairement dans l'intérêt public, ou en cas d'autorisation par la loi, ces renseignements ne doivent être recueillis, employés et divulgués qu'avec le consentement explicite et éclairé des personnes visées.
- L'un des principes de base de la vie privée est le droit d'être laissé seul. Il faut instaurer un équilibre entre l'usage légitime des télécommunications non sollicitées et leur potentiel d'intrusion dans la vie privée personnelle. Toutes les parties en cause doivent établir des règles de base ainsi que des méthodes de compensation afin que les Canadiens puissent se protéger contre les télécommunications indésirables et intrusives.
- Les attentes des Canadiens en ce qui concerne leur vie privée peuvent changer avec le temps. Les méthodes de protection de la vie privée en matière de télécommunications doivent être révisées de temps à autre en fonction de ces nouvelles attentes ainsi que de l'évolution de la technologie et des services.

B — Les lignes directrices de l'OCDE et le projet de l'Association canadienne de normalisation sur l'élaboration d'une norme sur la protection de la vie privée

Établies à la fin des années 70 et adoptées sous forme d'une recommandation du Conseil de l'OCDE en septembre 1980, les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel ont constitué une base de saines pratiques d'information à l'époque, et représentent une réalisation remarquable pour un groupe de pays largement dépourvus de lois sur la protection des données. Néanmoins, les Lignes directrices exigeront peut-être d'autres précisions dans le cadre de la technologie du XXI[e] siècle. Les concepts visés se retrouvent dans les principes ci-dessous :

- Huit principes fondamentaux applicables sur le plan national sont exposés à la Partie deux des Lignes directrices. Ils portent sur la limitation en matière de collecte, la qualité des données, la précision des finalités, la limitation de l'utilisation, les garanties de sécurité, la transparence, la participation et la responsabilité individuelles.
- Quatre principes applicables sur le plan international, portant sur la libre circulation et les restrictions légitimes, sont exposés à la Partie trois des Lignes directrices.

Lorsque l'Association canadienne de normalisation a élaboré son code modèle sur la vie privée, elle s'est inspirée des Lignes directrices de l'OCDE, les interprétant dans le contexte canadien de 1991. Il est important d'évaluer la norme de l'Association dans son entier, étant donné que le commentaire sur les principes est important pour la compréhension de chacun de ces derniers. Cependant, étant donné que le projet n'est pas encore soumis à l'examen public, les 10 principes ne sont que brièvement exposés ci-après, accompagnés d'une explication lorsqu'ils sont différents des Lignes directrices de l'OCDE. Le public sera invité à commenter la version finale, à l'automne de 1994.

1. Responsabilité (considérée comme fondamentale au point d'être le premier principe)
2. Énoncé des finalités
3. Consentement (nouveau)
4. Limitation en matière de collecte
5. Limitation de l'usage, de la divulgation ou de la conservation
6. Exactitude
7. Garanties
8. Transparence
9. Accès individuel
10. Refus de conformité (nouveau; donne au particulier le droit de contester la conformité d'un organisme à l'un ou à l'autre des principes, et non seulement l'exactitude des données touchant le particulier).

1987 Le Comité permanent de la justice présente son rapport examinant l'application de la *Loi sur la protection des renseignements personnels* et critiquant l'absence de conformité du secteur privé aux Lignes directrices de l'OCDE ainsi que l'inertie gouvernementale.

1990 La Communauté européenne présente des projets de directives sur la protection des données en général ainsi qu'en matière de télécommunications; les États-Unis et des intervenants de l'étranger entament des démarches dynamiques pour diminuer l'importance des aspects de la directive sur les flux transfrontières de données et pour diminuer les aspects restrictifs pour le commerce.

1991 L'OCDE remanie le concept de protection des données; la Communauté européenne cherche à protéger ses directives sur la vie privée dans l'Accord général sur les tarifs douaniers et le commerce.

1991 Les principaux ministères fédéraux, de même que l'industrie et des groupes de consommateurs, appuient la demande présentée par l'Association canadienne de normalisation pour élaborer un code de pratique modèle fondé sur l'OCDE.

1992 Le ministère des Communications présente les *Principes de protection de la vie privée dans les télécommunications,* et rédige un projet de loi sur la protection des communications par téléphones cellulaires.

1993 La nouvelle *Loi sur les télécommunications* est adoptée par le gouvernement fédéral et entre en vigueur le 25 octobre 1993; elle donne au CRTC un mandat précis visant à protéger la vie privée dans les télécommunications, et lui confère des pouvoirs étendus à cette fin.

1993 Le Québec adopte le projet de loi 68 sur la protection des renseignements personnels dans le secteur privé, qui est devenu loi le 1er janvier 1994.

Annexes

A — Chronologie des activités

La question de la vie privée dans une économie fondée sur l'information s'est posée à l'échelle mondiale dans les années 70. Au Canada, l'ancien ministère des Communications s'est joint au ministère de la Justice pour former un groupe d'études sur les ordinateurs et la vie privée, groupe qui a préparé plusieurs études, notamment un rapport intitulé *Les ordinateurs et la vie privée* (Ottawa, Information Canada, 1972). L'OCDE, pour sa part, considérait la protection de la vie privée comme touchant les flux transfrontières de données, et les pays membres ont constaté qu'ils avaient mutuellement intérêt à protéger la vie privée et les libertés individuelles ainsi qu'à concilier les valeurs fondamentales mais concurrentielles de la vie privée et de la libre circulation de l'information. On a reconnu que les flux transfrontières de données à caractère personnel contribuent au développement socio-économique et que des restrictions en la matière pourraient nuire aux activités de multinationales et perturber gravement des secteurs économiques importants comme les banques, les assurances et les voyages. L'OCDE a promulgué les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel. Vers la même époque, le Conseil de l'Europe adoptait un document similaire, la Convention 108, auquel les pays européens ont réagi de façon très différente sur le plan législatif. C'est la lenteur des membres à intervenir qui a incité la Communauté européenne à introduire des directives plus strictes ayant force de loi.

Voici les principaux événements et intervenants, dans l'ordre chronologique :

1969 L'OCDE reconnaît les répercussions des flux transfrontières de données sur la vie privée; un groupe de spécialistes est constitué en 1978.

1970 Les États-Unis adoptent le *Fair Credit Reporting Act.*

1972 Le groupe d'études Justice-Communications présente son rapport sur les ordinateurs et la vie privée.

1977 Le poste de Commissaire à la protection de la vie privée est établi en vertu de la *Loi canadienne sur les droits de la personne.*

1980 L'OCDE promulgue les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel.

1981 Un groupe de travail interministériel sur les flux transfrontières de données est créé au Canada.

1982 Le Conseil de l'Europe adopte la Convention 108 sur la protection des données; le Canada adopte la *Loi sur la protection des renseignements personnels,* pour les dossiers relevant de l'administration fédérale.

1984 Le Canada signe les Lignes directrices de l'OCDE; le ministère de la Justice est chargé d'inciter l'industrie à se conformer rapidement à ce document.

Commentaires publics

Ce document vise à contribuer au débat sur les répercussions socio-économiques de l'autoroute de l'information, et non à proposer des solutions définitives. Les particuliers et les organismes publics et privés sont invités à nous faire part de leurs vues. Ils sont priés de faire parvenir par écrit leurs commentaires sur les démarches en la matière, les questions suivantes ou tout autre aspect du présent document de travail. Se référer à l'adresse indiquée dans la préface.

- Quels principes devraient être à la base d'une protection efficace de la vie privée ?
- Le gouvernement doit-il introduire des mesures plus fermes pour protéger la vie privée et la sécurité de l'information ? Comment peut-on utiliser efficacement chacune des quatre démarches décrites ci-dessus ?
- Faut-il instaurer une protection à l'échelle nationale ou au contraire faire confiance à une réglementation provinciale ou sectorielle ?
- Dans quelles circonstances conviendrait-il de recourir à des lignes directrices volontaires sur la vie privée préparées par le monde des affaires ?
- L'autoroute de l'information devrait-elle être conçue pour assurer un niveau élevé de protection ou, au contraire, une telle structure ralentirait-elle le rythme et ferait-elle augmenter le coût de l'innovation ?
- Comment les Canadiens peuvent-ils participer davantage au processus de conception de techniques et de services susceptibles de menacer la vie privée ?
- Comment les Canadiens peuvent-ils se renseigner davantage sur la valeur de leurs renseignements personnels et sur la nécessité d'en contrôler l'utilisation ? Quel rôle le monde des affaires et les pouvoirs publics doivent-ils jouer dans l'éducation du public ?

La technologie établie sur le marché peut avoir de grandes répercussions sur les droits des consommateurs, mais comment ceux-ci peuvent-ils modifier le processus de mise au point technologique ? Devrait-il y avoir des audiences publiques, comme celles du CRTC pour les services de télécommunications, lorsqu'une nouvelle technologie arrive sur le marché ? Faudrait-il examiner au moyen de tribunes publiques les conséquences de tous les nouveaux systèmes et normes d'information sur la vie privée ? Incombe-t-il au gouvernement ou au marché de déterminer les niveaux de protection à offrir ? La vie privée devrait-elle être une option, que seuls certains Canadiens pourraient se permettre, ou n'entraîner aucun coût et être considérée comme inhérente aux services offerts ?

Éducation des consommateurs

Il est essentiel de sensibiliser le monde des affaires à la nécessité d'aborder de façon plus éclairée la manutention des données personnelles, et de sensibiliser les consommateurs aux façons de se protéger. Les consommateurs ont besoin de renseignements et d'éducation sur leurs droits, la valeur de leurs renseignements personnels, les risques présentés par la nouvelle technologie à leur vie privée et les mesures qu'ils peuvent prendre pour préserver cette dernière. Bien que la plupart des Canadiens considèrent la protection de la vie privée comme une responsabilité gouvernementale, voire celle d'un partenariat entre les pouvoirs publics et les entreprises, ils estiment que le particulier a un grand rôle à jouer pour résoudre les problèmes dans ce domaine. Comment les responsabilités devraient-elles être partagées ?

sanctions légales ? L'expérience avec des codes volontaires n'a pas été jusqu'ici encourageante, ceux-ci n'étant pas toujours conformes aux Lignes directrices de 1981 de l'OCDE. Selon la plupart des spécialistes en matière de vie privée, ces codes sont insuffisants pour parer aux risques des années 90.

Le projet de l'Association canadienne de normalisation sur l'élaboration d'une norme nationale sur la vie privée dépasse le cadre des codes volontaires. En définissant les principes de base de tout code, la norme apporte une solution au langage souvent faible et ambigu utilisé dans la rédaction des codes. Une protection similaire à celle d'une législation pourrait être assurée au moyen d'une vérification et d'une certification faites par un organisme de normalisation tel que le Quality Management Institute, une division de l'Association canadienne de normalisation. Il sera difficile de protéger efficacement la vie privée au moyen de la norme volontaire proposée par l'Association, si cette norme n'est pas adoptée entièrement et mise en œuvre dans toutes les associations industrielles et les entreprises.

On a aussi proposé des démarches contractuelles, selon lesquelles les consommateurs accepteraient que leurs données soient utilisées à des fins précises, peut-être en retour d'escomptes ou d'honoraires. Il faut veiller à ce qu'une telle démarche axée sur le marché ne réserve pas la protection de la vie privée aux riches. Actuellement, peu de gens comprennent la valeur marchande de leurs renseignements personnels ou savent comment les protéger. En outre, les contrats qui limitent ou suppriment les valeurs fondamentales de la vie privée sont susceptibles de devenir une pratique industrielle en l'absence de droits clairement définis.

Solutions technologiques

Une autre démarche consiste à utiliser la technologie pour protéger les données personnelles. Traditionnellement, la technologie a plutôt servi à augmenter le nombre des renseignements recueillis, de sorte que les partisans actifs de la vie privée ont plutôt tendance à s'en méfier. Cependant, la technologie en soi est neutre et peut servir à améliorer la vie privée autant qu'à la menacer. Il est possible de concevoir des techniques de manière que le réglage implicite corresponde à une absence de collecte de données. De même, des systèmes téléphoniques peuvent « oublier » les derniers chiffres d'un numéro de téléphone après un appel, afin de protéger la vie privée dans les énoncés de facturation personnelle. Des systèmes de courrier électronique peuvent fournir des messages éphémères pour usage personnel, au moyen d'une encre électronique qui s'estompe. La conception de l'autoroute de l'information devrait-elle améliorer la capacité d'une personne de contrôler ses renseignements personnels ainsi que transactionnels ?

Un domaine aussi important que mal étudié est le codage ou le chiffrement. Un codage fort peut maintenant être intégré à des logiciels, à des puces dans un équipement comme des postes téléphoniques ou de minuscules ordinateurs, ou encore être utilisé dans des cartes intelligentes. Ces dernières, grâce à un chiffrement à clé révélée, peuvent protéger l'identité ou les titres contre toute fraude, et permettre au détenteur de rester anonyme. La même technologie peut servir à se procurer des fonds d'une manière électronique et fiable, mais pratiquement impossible à retracer, ce qui est une méthode beaucoup plus sûre pour le consommateur que la diffusion d'un numéro de carte de crédit sur l'autoroute de l'information.

secteurs du marché placés sous juridiction fédérale. Comme cette démarche pourrait aggraver les disparités entre les entités réglementées et celles non réglementées, il faudrait collaborer avec d'autres autorités pour établir un ensemble de règles communes à tous les secteurs.

Une loi fédérale répondrait au désir exprimé par les Canadiens de voir instaurer une supervision gouvernementale de la protection des consommateurs. Elle pourrait aussi servir à amorcer un dialogue pour améliorer la protection de la vie privée aux niveaux provincial et territorial. Un cadre fédéral et un cadre provincial complémentaires réduiraient les préoccupations communes, dont la possibilité de barrières commerciales interprovinciales causées par des exigences ainsi que des pratiques en matière de protection de la vie privée variant d'une province ou d'un territoire à l'autre. La loi devrait permettre d'uniformiser les règles du jeu entre les entreprises concurrentielles et les consommateurs, et ce, d'un océan à l'autre. Le secteur privé est actuellement assujetti à divers régimes de réglementation. Ainsi, les clauses de protection de la vie privée contenues dans la *Loi sur les télécommunications* s'appliquent aux entreprises assujetties à une réglementation fédérale, mais non aux revendeurs de télécommunications ni aux fournisseurs de services d'information. Étant intégré dans le prix des biens et des services, le coût de la disparité des normes est assumé par les consommateurs.

De nombreux segments de la population favoriseraient une démarche législative. Le sondage canadien de 1992 sur le respect de la vie privée démontrait qu'une grande majorité de Canadiens était en faveur d'une législation gouvernementale ou d'un partenariat entre le secteur public et le secteur privé pour élaborer des lignes directrices à l'intention du secteur privé. Selon le rapport Equifax Canada sur les consommateurs et la vie privée à l'ère de l'information, publié en 1992, 84 p. 100 des cadres des compagnies d'assurances, des services financiers et des bureaux de crédit croient qu'une législation fédérale est nécessaire pour fixer des règles présidant à la collecte et à la circulation des renseignements sur les consommateurs et éviter ainsi un ensemble disparate de régimes provinciaux. Cette vue semble aller à l'encontre de la tendance actuelle vers la déréglementation et la réduction du contrôle gouvernemental, mais elle reconnaît peut-être que des règles de base harmonisées pour la protection des données profitent au commerce et peuvent être appliquées sans trop de bureaucratie. En effet, ces règles permettraient à tous les intervenants de soutenir la concurrence de manière équitable et susciteraient la confiance chez les consommateurs.

Codes et normes volontaires

Permettant aux diverses industries d'adapter leurs dispositifs de protection des données aux besoins de leurs clients, au milieu de réglementation où elles opèrent ainsi qu'aux exigences du marché, les codes volontaires sont la méthode préférée des gens d'affaires et des associations industrielles du Canada.

Il n'est pas nécessaire que les codes volontaires soient moins stricts que ceux imposés par la loi, mais c'est la question même du caractère exécutoire qui préoccupe les défenseurs des consommateurs. Qui est responsable en fin de compte ? A qui un consommateur lésé doit-il s'adresser pour obtenir réparation ? Étant donné que la valeur des renseignements personnels augmente en fonction d'une économie de plus en plus axée sur l'information, comment assurer la protection de ces renseignements sans l'aide de

5 Les démarches possibles pour le Canada

La plupart des Canadiens doutent de leur capacité de protéger leur vie privée, et croient que cette responsabilité incombe aux pouvoirs publics ou à un partenariat entre le secteur public et le monde des affaires. La mise au point de l'autoroute de l'information encouragera sûrement le débat sur ces questions et les demandes d'intervention.

Parmi les démarches possibles pour protéger la vie privée, notons les lois, une norme nationale et volontaire améliorée sur la vie privée, la promotion de techniques comme le codage et les cartes intelligentes ainsi que l'éducation des consommateurs. Le Canada devra peut-être recourir à toutes ces solutions.

Lois et réglementation

L'énorme réserve de renseignements détenus par les autorités (dossiers médicaux et fiscaux, dossiers d'assistance sociale, d'immigration et de police), est protégée à un certain point au niveau fédéral et au Québec, en Ontario, en Saskatchewan, en Colombie-Britannique et en Alberta. La qualité de la protection varie d'un secteur de compétence à l'autre; de plus, lorsque l'information se déplace, on ne sait pas toujours par quelle loi elle est régie. Constatant cette situation dans son rapport de 1993-1994, le Commissariat à la protection de la vie privée décrivait la protection au Canada comme une mosaïque d'initiatives publiques et privées qui abordent le sujet de façon disparate. Le commissaire prônait l'adoption d'une loi nationale sur la protection de la vie privée pour établir les principes et le cadre de cette protection, à la fois pour le monde des affaires et pour le secteur public. Les commissaires provinciaux et les gouvernements ayant eux aussi reconnu ces problèmes, il est peut-être temps d'entamer un dialogue pour trouver des solutions.

Bien qu'une loi fédérale soit souhaitable pour assurer une protection et des droits uniformes dans tout le Canada, la séparation des pouvoirs entre les secteurs de compétence fédéraux et provinciaux est un obstacle. Le gouvernement fédéral a le pouvoir nécessaire pour réglementer des industries comme les télécommunications, les transporteurs et les banques. Toutefois, les provinces exercent des responsabilités dans les transactions individuelles entre consommateurs et le commerce au détail. En modifiant les lois sectorielles actuelles, le gouvernement fédéral pourrait créer des exigences en matière de protection de la vie privée dans chaque secteur réglementé. Une autre option serait d'appliquer la *Loi sur la protection des renseignements personnels* à tous les

d'examiner leurs fichiers et de corriger les erreurs. En 1974, la loi fédérale *Privacy Act* était adoptée pour protéger la vie privée des particuliers en ce qui concerne les renseignements contenus dans les registres de l'administration fédérale et susceptibles d'être divulgués en vertu du nouveau *Freedom of Information Act*. On insistait cependant sur cette dernière et l'on ne prévoyait aucune surveillance indépendante de l'application de la *Privacy Act*. Pour parer aux scandales dans le monde du crédit, les États-Unis révisent actuellement leurs lois sur les rapports équitables en matière de crédit.

Ce pays réexaminent aussi la protection de la vie privée dans le contexte de l'initiative National Information Infrastructure (NII), se rapprochant des démarches du Canada pour demander des conseils sur la nature souhaitable de la future autoroute de l'information. Les États-Unis ont constitué un groupe de travail chargé d'examiner uniquement les questions relatives à la vie privée. Ce groupe a présenté des principes aux fins de commentaires, mais n'a pas encore prévu de mécanismes de supervision. La National Telecommunications and Information Agency, service du Department of Commerce chargé des conseils sur les politiques relatives à la NII, a lancé un appel pour recueillir des commentaires sur les conséquences des services de télécommunications sur la vie privée, et a publié un document de travail traitant de questions touchant les renseignements relatifs aux transactions.

La protection de la vie privée dans d'autres pays

L'Europe privilégie des règlements généraux sur la protection des données, applicables aux secteurs public et privé, et supervisés par des commissaires indépendants chargés des données. Les pays dont l'histoire les a sensibilisé aux questions de protection des données (Allemagne, France, Autriche, Suède) ont adopté des lois au cours des années 70. A la fin de cette décennie, il existait sur ce continent un tel déséquilibre dans ce domaine que le Conseil de l'Europe amorça des pourparlers sur une convention qui obligerait les pays membres à adopter des lois similaires. En 1981, l'OCDE élaborait ses Lignes directrices pour assurer le même type d'harmonisation parmi ses États membres, craignant que la disparité dans la protection des droits de la vie privée n'incite les pays protégeant les données à bloquer le flux de ces dernières vers les nations plus laxistes. A la fin des années 80, bon nombre de pays européens n'avaient toujours pas émis de lois sur la protection des données même s'ils y étaient obligés par la Convention 108 du Conseil de l'Europe. La Commission des Communautés européennes, inquiète à l'idée que les commissaires chargés des données pouvaient bloquer des transferts entre les pays et ainsi nuire au développement d'un marché européen commun, passa à l'action.

En 1990, elle publiait deux projets de directives sur la protection des données qui, si elles sont adoptées par le Parlement européen, auront force de loi. La première, une directive générale sur toutes les données personnelles, informatisées ou manuelles, interdisait le flux de données vers les pays dépourvus d'une protection adéquate. La deuxième, très structurée, portait sur la vie privée en matière de télécommunications et dictait les mesures précises que devraient prendre les pays membres ainsi que les partenaires commerciaux contre les intrusions suscitées par l'identification des appelants, les téléphones cellulaires et à haut-parleur ainsi que l'enregistrement des données d'appels. Bon nombre d'entreprises et de pays membres se sont vite opposés à divers aspects de la directive. En 1992, la principale directive réapparaissait avec une extraterritorialité largement réduite; une version ultérieure sera sans doute adoptée d'ici la fin de 1994.

Les États-Unis, pour leur part, ont tendance à se fonder sur des codes de pratique volontaires et des lois sectorielles. En 1970, ils adoptaient le premier *Fair Credit Reporting Act*, reconnaissant que les profils détaillés nécessaires aux activités de crédit devaient être compensés par la possibilité, pour les consommateurs,

prolifération du télémarketing et de la publicité importune par télécopieur, le gouvernement fédéral a annoncé, en décembre 1992, des principes de protection de la vie privée dans les télécommunications (voir annexe C). Ces principes visaient à sensibiliser l'industrie aux préoccupations sur la vie privée ainsi qu'à promouvoir une démarche fondée sur l'autoréglementation. Ils renforcent les droits des particuliers à contrôler leurs renseignements personnels et à se renseigner sur les répercussions que peuvent avoir, sur leur vie privée, les nouveaux produits et services de communications ainsi que d'information. Bien que le projet d'agence de protection de la vie privée en matière de télécommunications, proposé pour superviser la mise en œuvre de ces principes, ne se soit jamais concrétisé, les principes ont influé sur l'élaboration de codes volontaires dans le secteur des télécommunications.

La nouvelle *Loi sur les télécommunications*, entrée en vigueur en octobre 1993, donne au CRTC des pouvoirs accrus pour protéger la vie privée des particuliers et réglementer les communications non sollicitées. Le gouvernement a aussi introduit des modifications au Code criminel ainsi qu'à la *Loi sur la radiocommunication*, entrés en vigueur en août 1993 et interdisant la divulgation des communications téléphoniques radio interceptées.

En plus de ces initiatives sectorielles, le Canada fait l'essai d'un code type national plus complet. A l'automne 1990, l'Association canadienne de normalisation a commencé à élaborer une norme nationale sur la vie privée, qui pourrait s'appliquer à tous les secteurs et à toutes les provinces. Plusieurs ministères fédéraux, des intervenants clés du secteur privé et divers représentants des consommateurs participent à cette initiative. Un projet devrait être présenté au public à la fin de 1994. Une démarche normalisée de la protection des données pourrait permettre d'examiner la question de la vie privée pendant la mise au point de techniques d'information et de communications, et l'on pourrait en faire la promotion auprès des partenaires commerciaux à l'étranger. Une norme élaborée au Canada pourrait être incluse dans les normes de gestion de la qualité de l'Association internationale de normalisation (série ISO 9000) pour inciter les grandes entreprises à traiter la gestion des données personnelles de la même façon que la sécurité, la gestion des salles blanches et d'autres mécanismes de contrôle de la qualité.

Les pouvoirs des commissaires ou des ombudsmans provinciaux varient. Ainsi, le commissaire de la Colombie-Britannique peut émettre des arrêts exécutoires, tandis que celui de l'Ontario formule des recommandations. Seul celui du Québec exerce une juridiction sur le secteur privé, auquel il peut imposer, en cas de dérogation, des amendes allant jusqu'à 20 000 $.

Au Québec, la question de la vie privée a été examinée différemment, surtout parce que le Code civil prévoit un droit spécifique et détaillé à la vie privée, lequel englobe les renseignements privés aussi bien que publics. Le Québec est allé plus loin que toutes les autres provinces en adoptant une loi protégeant tous les renseignements personnels détenus tant par le secteur public que par le secteur privé. Entrée en vigueur en janvier 1994, cette loi est l'une des premières du genre à être appliquée hors de l'Europe et a déjà incité les organismes nationaux à se fonder sur les mêmes normes.

La protection dans le secteur privé

Hormis cette initiative au Québec, l'utilisation croissante des renseignements personnels et leur gestion dans le secteur privé sont très peu réglementés au Canada. Certains secteurs ont pourtant volontairement tenté d'établir et de mettre en œuvre des codes équitables sur l'information ou la vie privée. Ces codes tentent de définir les limites et d'établir des lignes directrices pour la protection des renseignements personnels afin d'instaurer un équilibre entre les avantages socio-économiques et le droit d'une personne de contrôler les renseignements qui la concernent.

L'Association canadienne du marketing direct a un code volontaire qui offre aux consommateurs la possibilité de déroger au processus ou de refuser que leurs données soient transmises ou vendues à d'autres entreprises. Elle enjoint ses membres d'aider les consommateurs à déceler les informations erronées qui se seraient glissées dans leurs dossiers.

Depuis 1991, le secteur des opérations bancaires dispose d'un code sur la vie privée. Son contenu et son application n'ont cependant pas été conformes aux attentes des défenseurs de la vie privée, surtout pour ce qui est de l'accès du client aux renseignements personnels et du nombre de renseignements requis pour accorder un crédit. Dans des audiences publiques tenues en 1993, le Sénat canadien a étudié un projet de règlement qui porterait sur les préoccupations des banques dans le cas où le ministre des Finances réglementerait ce secteur. Il n'y a toutefois eu aucun appel officiel pour concrétiser cette proposition.

Le secteur des télécommunications présente un mélange de méthodes volontaires et de réglementation. L'introduction de services d'identification de l'appelant, soit l'affichage du numéro de téléphone de ce dernier, a été critiquée par une forte coalition de citoyens inquiets — depuis les responsables de refuges pour femmes jusqu'aux foyers pour personnes âgées — pour son intrusion inhérente dans la vie privée. Le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) a obligé les compagnies de téléphone à offrir gratuitement un blocage par appel et un blocage de ligne aux personnes ayant des besoins spéciaux. Les médias se sont aussi largement intéressés au caractère privé des conversations par téléphones cellulaires et mobiles après que des entretiens privés de personnalités publiques aient été enregistrés au moyen d'appareils de balayage électronique. En réponse à ces préoccupations ainsi qu'à la

La protection de la vie privée au Canada

Depuis 20 ans, la législation sur la protection des données dans les pays industrialisés reflète les efforts déployés pour établir un équilibre entre, d'une part, ce que les pays démocratiques considèrent comme le droit fondamental à la vie privée et, d'autre part, la nécessité pour les pouvoirs publics et les entreprises d'obtenir des renseignements personnels permettant aux particuliers de participer à une société universelle complexe (voir annexe A). Des codes sur les pratiques équitables en matière d'information limitent la collecte de renseignements et donnent au particulier le droit d'accéder aux données qui le concernent, d'en contester l'exactitude et de corriger les erreurs, le cas échéant. Au cours des années 70, l'Organisation de coopération et de développement économiques (OCDE) a reconnu la nécessité d'examiner la question de la vie privée dans le contexte du flux croissant de données transfrontières. Les pays membres, dont le Canada, ont commencé à élaborer des lignes directrices. En 1981, l'OCDE a diffusé ses Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel (voir annexe B). Le Canada et d'autres pays membres ont adopté ces lignes directrices et ont indiqué qu'ils aborderaient les questions relatives à la vie privée, soit en adoptant des lois intégrant les principes en question, soit en instaurant des systèmes volontaires permettant de leur donner du poids.

La protection dans le secteur public

Le Canada emploie un ensemble de lois et de codes volontaires pour protéger la vie privée, applicables notamment aux renseignements personnels détenus par le gouvernement fédéral, certains gouvernements provinciaux et certaines municipalités. Fondée sur les Lignes directrices de l'OCDE, la *Loi sur la protection des renseignements personnels,* de 1982, protège l'information détenue par le gouvernement fédéral. Le Commissariat à la protection de la vie privée a été créé pour surveiller la façon dont le gouvernement fédéral recueille, utilise et divulgue les renseignements personnels sur ses clients et ses employés, et sur la façon dont il traite les demandes de consultation de dossiers personnels. Dans les rapports annuels au Parlement, les commissaires à la protection de la vie privée n'ont pas limité leurs commentaires à la protection des données au sein du gouvernement fédéral, mais ont examiné les tendances qui existent dans toute la société canadienne. Ces activités ont grandement servi la cause de la protection de la vie privée.

Certaines provinces ont emboîté le pas et ont adopté des lois exhaustives : le Québec, en 1982, l'Ontario, en 1987, la Saskatchewan, en 1991, la Colombie-Britannique, en 1992, l'Alberta, en 1994. La Nouvelle-Écosse a présenté en 1993 un projet de loi sur la protection de la vie privée pour le secteur public provincial.

Le télétravail ou travail à domicile présente aussi un risque de surveillance accrue. Les gestionnaires désireront peut-être mesurer la productivité des employés qui travaillent à domicile, en comptant les frappes de clavier, en mesurant la durée des appels téléphoniques ou en branchant des caméras vidéo au réseau. Ces techniques sont déjà utilisées dans certains secteurs de travail spécialisés. Quelles limites, si besoin est, faut-il imposer à une telle surveillance ? Une réglementation gouvernementale s'imposera-t-elle, ou suffira-t-il d'encourager un bon comportement et de justes pratiques contractuelles ?

L'autoroute de l'information promet de favoriser les opérations bancaires, le télétravail, la gestion des services publics et des appareils électroménagers ainsi que des activités de surveillance au foyer. Cela soulève de graves questions, non seulement sur la sécurité des données comprises dans le réseau, mais aussi sur la sécurité dans un logement, où un intrus pourrait pénétrer et forcer le propriétaire, par le biais de son ordinateur, à retirer de l'argent ou à créditer des fonds à un autre compte. Les systèmes de surveillance et de protection de domiciles offrent une garantie contre les voleurs et les incendies, mais dans quelle mesure doit-on leur confier des renseignements personnels ? Faut-il accepter qu'un flux de données vidéo sur chaque entrée et fenêtre de son domicile soit transmis à une compagnie de sécurité ou au service de police ? Comment contrôler la collecte, l'usage, la disponibilité, voire la revente de l'information recueillie sur l'utilisation des différents services à domicile ?

La technologie des satellites applicable aux téléphones mobiles dans le monde entier fournit une autre catégorie de renseignements personnels. Bientôt un numéro de téléphone unique et individuel se déplacera avec chacun, du lieu de travail au domicile, au chalet, à l'appartement d'un ami ou en voyage. Grâce à une technologie conventionnelle de radio et à hyperfréquences, des systèmes cellulaires locaux et d'autres services de communications personnelles permettront de retracer les conversations téléphoniques. Bien que très commode, cette situation signifie que l'ordinateur devra toujours savoir exactement où se trouve la personne. Les défenseurs du droit à la vie privée voudront savoir qui contrôlera l'information sur les allées et venues, pendant combien de temps cette information sera conservée et jusqu'où s'étendra cette laisse électronique. Dans une telle forme de surveillance et dans le cadre de méthodes semblables, comment établir un équilibre entre les intérêts des employés et ceux des employeurs ?

Intrusion

Les citoyens souhaiteront aussi être protégés contre les communications indésirables à la suite d'un achat fait par l'intermédiaire de l'autoroute de l'information. Les intrusions par les télévendeurs ou par le courrier publicitaire ciblé dérangent bon nombre de Canadiens. Déjà, des sollicitations importunes par télécopieur sont reçues pour tout genre de services, de la vente de café aux voyages d'agrément. Faut-il contrôler les programmes de commercialisation ciblés qui découlent d'achats séparés ou connexes (par exemple, les sollicitations envoyées par courrier électronique après l'achat d'un voyage dans les Caraïbes et qui proposent d'autres voyages) ? Dans l'affirmative, comment ? Quelles règles devraient régir la collecte et l'utilisation de l'information sur nos achats ou sur d'autres transactions personnelles ? Comment instaurer un équilibre entre ces règles et les possibilités d'être renseignés sur les biens ou services voulus ?

pourraient être codés sur la carte, ou encore les données pourraient être liées à un identificateur biométrique comme l'empreinte du pouce ou l'empreinte rétinienne. Étant donné le nombre actuel de fraudes commises au moyen de systèmes d'autorisation par cartes — qu'il s'agisse de cartes de crédit, de cartes d'appel ou de cartes santé — une pression de plus en plus forte s'exerce en faveur d'un système d'identification plus fiable. Les défenseurs du droit à la vie privée craignent toutefois que ces cartes ne facilitent un couplage inacceptable des données, ou la création d'une société où il serait obligatoire de porter en tout temps des documents d'identité sur soi. Le public souhaitant vivement une diminution des fraudes qui grèvent nos programmes sociaux, où se trouve l'équilibre entre, d'une part, une administration responsable des programmes et services et, d'autre part, une érosion inacceptable des libertés individuelles et du droit à la vie privée ? Un numéro identificateur unique accroît la capacité de recueillir et d'assortir des renseignements personnels. Devrait-il y avoir des limites à ces identificateurs ?

Dans le domaine de l'information sur la santé, la vie privée est une question délicate. Les médecins, les cliniques et les hôpitaux, les assureurs et les pouvoirs publics, les épidémiologistes et les chercheurs s'intéressent aux besoins médicaux pour des motifs différents, et pourraient vouloir accéder à des données sur la vie d'une personne pour des raisons très valables. Cependant, les particuliers, tout aussi légitimement, craignent que les fournisseurs d'avantages ou les employeurs n'abusent de cette information. Sur une carte santé intelligente mise à l'essai au Québec, les renseignements ont été stockés sur quatre quadrants; chaque fournisseur de service (par exemple, une pharmacie) n'avait accès qu'à l'information qui le concernait. Cette solution résout le problème que pose l'accès de tous les intervenants dans le système médical à la gamme complète de données, mais ne règle pas la question fondamentale posée par une technologie qui favorise la création de fichiers de la naissance à la mort et l'intrusion dans la vie privée que cela signifie.

Surveillance et contrôle

Les styles de vie, les régimes de travail et les transactions commerciales seront transformés à mesure que le pouvoir de l'informatique et des réseaux pénétrera dans chaque domicile et entreprise. Bien que chacune des techniques de l'information présente des caractéristiques différentes, elles contribuent toutes à établir une capacité sans précédent de surveillance de chaque homme, femme et enfant, qu'il s'agisse d'un client, d'un étudiant, d'un employé, d'un patient, d'un contribuable ou d'un bénéficiaire de services gouvernementaux.

L'une des applications les plus communes des réseaux informatiques est le courrier électronique. L'efficience et la commodité de ce nouveau système d'information lui ont valu une popularité instantanée dans les secteurs tant commerciaux que sociaux. Le courrier électronique d'un employé devrait-il être traité comme une lettre privée ou au contraire comme un bien appartenant à une entreprise et, par conséquent, susceptible d'être lu par un opérateur de système ou par un superviseur ? Ces systèmes devraient-ils être conçus pour faciliter le codage ou le chiffrement des messages, pour les protéger contre l'envoi et la diffusion par inadvertance de messages confidentiels ? Tout comme ont été élaborées des conventions et une étiquette pour la manipulation du courrier personnel et d'affaires à travers les siècles, faudrait-il adapter ces normes au nouveau milieu électronique ?

des soins médicaux, ou la citoyenneté canadienne), limitant leurs chances et annulant les progrès de la société en matière d'équité et de droits de la personne. Sur un marché du travail très concurrentiel, où des milliers de personnes envoient des curriculum vitæ même pour de modestes emplois, quel genre de présélection à partir de bases de données sommes-nous disposés à accepter ? Comment les postulants non retenus pourront-ils s'assurer que leur candidature n'a pas été rejetée à cause d'une information erronée qui figurait dans leur fichier ? Les organismes devraient-ils être tenus de communiquer aux particuliers les renseignements détenus à leur sujet, et de leur fournir, à peu de frais ou gratuitement, un accès à ces fichiers aux fins de vérification ou de correction ? Devrait-on imposer des limites de temps au stockage de l'information ?

La prestation de nouveaux services par l'intermédiaire de l'autoroute de l'information, tels la vidéo sur demande, les magazines et les catalogues électroniques, permettra de recueillir des renseignements encore plus variés sur les intérêts et les choix de certaines personnes en matière de divertissement et de lectures. Faut-il établir une réglementation pour limiter le stockage et l'utilisation de ces données détaillées, ainsi que l'accès à celles-ci ? Y a-t-il un danger à permettre à ces systèmes de recueillir des renseignements sur nos habitudes, même à des fins anodines ? Comment peut-on protéger les droits individuels à la vie privée pendant les différentes étapes de la collecte, du stockage et de l'échange de l'information ? Devrait-on exiger un consentement donné en toute connaissance de cause pour les différentes activités et transactions en matière d'information qu'un organisme peut entreprendre en utilisant des renseignements personnels ?

Sécurité transactionnelle et identification individuelle

Bien que l'on puisse protéger le contenu d'un message électronique par codage ou chiffrement, la vérification de l'identité d'un expéditeur et d'un destinataire constitue un élément critique de la protection de la vie privée, notamment pour les échanges de renseignements financiers et commerciaux ou pour l'envoi de renseignements confidentiels. Les transactions ordinaires se font de moins en moins souvent en personne, mais plutôt au moyen du téléphone, du télécopieur ou de commandes par catalogues. Les méthodes actuelles d'authentification et de paiement exigent divers types de renseignements personnels qui ne sont pas facilement connus, depuis le numéro de carte de crédit jusqu'au nom de jeune fille de la mère d'une personne donnée. La possibilité, pour les consommateurs, d'effectuer des transactions commerciales par voie électronique à partir de leur domicile pose de nouveaux défis. Comment vérifier l'identité ou la solvabilité d'une personne qui passe une commande électronique ou demande la livraison de dossiers médicaux ? Est-ce que les méthodes actuelles d'authentification suffiront sur l'autoroute de l'information ? D'autres méthodes, telles les signatures numériques, seraient-elles plus sûres ?

Cartes d'identité et numéros identificateurs uniques

Un autre aspect du débat sur la vie privée est l'émission de cartes d'identité. La nouvelle technologie relative aux cartes intelligentes donne aux organismes les moyens de dépasser les capacités actuelles de stockage sur les bandes magnétiques, pour accéder à l'énorme potentiel de stockage des puces intégrées. Des renseignements détaillés sur une personne, voire des photos,

2 Les effets de l'autoroute de l'information sur la vie privée

Données transactionnelles et profils personnels

La collecte de données transactionnelles deviendra beaucoup plus facile dans un monde informatisé et maillé. Les grands progrès réalisés quant à la capacité des ordinateurs, la liaison d'un grand nombre d'entreprises par des systèmes de paiement électronique, et le maillage complet des bases de données sur les ventes et les commandes ont révolutionné la relation entre les consommateurs et les producteurs de biens et de services. Grâce à la gestion de l'approvisionnement « juste-à-temps », les producteurs fabriquent et expédient les biens aux entrepôts et aux fournisseurs selon l'information reçue des terminaux situés aux points de vente de leurs clients. Les grossistes et les détaillants se raccordent de plus en plus à cette chaîne. Le lien entre une personne et un achat particulier n'est qu'un maillon de plus de la chaîne, qui facilite la commercialisation directe et l'analyse de marché. La plupart des gens savent qu'un établissement émetteur de cartes de crédit peut vendre les données transactionnelles qui les concernent à des fournisseurs de produits, mais ils peuvent considérer ce risque comme un inconvénient raisonnable compensé par l'avantage du recours à un établissement de crédit important et fiable. Dans le nouveau milieu maillé, toutes les entreprises, grandes ou petites, fiables ou non, seront en mesure de constituer des fichiers de données sur leur clientèle ou d'acheter des bases de données sur les clients auprès d'autres fournisseurs. Quel est le meilleur équilibre entre les avantages sociaux et commerciaux d'une technologie aussi avancée et les dangers qu'elle représente pour la protection de la vie privée ? Quels contrôles et quelles mesures de protection faut-il imposer quant à l'utilisation et à la réutilisation de cette information ?

L'autoroute de l'information pourrait grandement faciliter l'établissement du profil des personnes en fonction de leurs besoins, de leur style de vie ou de leurs choix d'achats. Cela pourrait avoir des répercussions malencontreuses si ces profils servaient à empêcher les personnes, et ce, à leur insu, de saisir les occasions qui s'offrent à elles. Le stockage dans des bases de données et les rapprochements des renseignements permettraient de prendre des décisions sur des particuliers, ce qui modifierait les conditions d'accès à divers produits, services et perspectives d'emploi. Cette situation pourrait pénaliser les personnes déjà vulnérables (malades, personnes âgées ou chômeurs, celles qui cherchent à obtenir des prestations d'aide sociale,

Qu'est-ce que la vie privée ?

La vie privée est normalement définie de deux façons : le droit de vivre en paix, sans intrusion ni interruption, et le droit de contrôler les renseignements qui touchent sa personne.

Les Canadiens accordent une grande importance au droit de vivre en paix, sans être dérangés. C'est le droit à la solitude, à l'anonymat, au partage de son temps avec des personnes choisies, ainsi que le droit de définir son espace et ses frontières. Ce concept englobe plusieurs questions qui dépassent l'acquisition et la diffusion de renseignements personnels. Bien que la *Charte canadienne des droits et libertés* ne contienne aucun droit spécifique en matière de vie privée, elle garantit à une personne, dans ses rapports avec le gouvernement, le droit à la vie, à la liberté et à la sécurité personnelles ainsi que le droit à la protection contre une fouille et une saisie déraisonnables. Bon nombre de spécialistes doutent cependant de l'efficacité de la protection offerte par la Charte.

Par protection des données personnelles, on entend la revendication, par des personnes, du droit de déterminer quand, comment et dans quelle mesure des renseignements qui les concernent sont communiqués à autrui. La protection des données est un aspect de la protection de la vie privée qui comprend le contrôle exercé sur la collecte, le stockage, l'exactitude, l'utilisation et la diffusion de renseignements personnels.

La grande mobilité dont jouissent les Canadiens les amènent à être connus de diverses personnes non pas personnellement, mais par le biais des informations disponibles à leur sujet. Quand nous voyageons, effectuons des emplettes, obtenons des services, conduisons un véhicule ou communiquons à partir de différents emplacements, notre identité et nos droits doivent être bien définis. Les fournisseurs de services de tous genres demandent des renseignements détaillés permettant de vérifier notre identité et de confirmer notre capacité de payer. Simultanément, ces renseignements et les données laissées par les transactions électroniques permettent de prévoir les possibilités de commercialisation, et donc incitent les personnes à conserver ces renseignements personnels dans des banques de données. L'échange et la commercialisation de renseignements personnels sont de plus en plus répandus dans le monde. La protection des données devient donc l'élément clé de la protection de la vie privée.

Dans le « réseau de réseaux », le Canada forme un maillon de la « chaîne d'information » internationale ou du « village planétaire ». A titre de nation souveraine, il a pris des engagements à l'échelle internationale, dans le cadre de divers traités et conventions; à titre de nation commerciale et de chef de file en technologie et en télécommunications, le Canada s'intéresse à la façon dont d'autres pays réagissent face aux défis que suscite la protection de la vie privée. Ce document traite aussi de la participation canadienne à des organismes internationaux soucieux de protéger la vie privée, ainsi que des efforts déployés par certains des partenaires commerciaux du Canada dans ce domaine. Enfin, diverses méthodes sont proposées pour étendre la protection des données et de la vie privée au Canada.

Introduction

Les entreprises, les organismes publics et les administrations publiques rassemblent, stockent, transmettent et échangent un grand nombre de renseignements personnels et professionnels, sous forme imprimée ou électronique. Le passage à l'interaction informatisée et l'interconnexion de réseaux augmentent le nombre de renseignements pouvant former le profil d'un individu. Ces données peuvent être envoyées à l'étranger, vendues ou réutilisées; elles peuvent être intégrées à des bases de données autres que celles pour lesquelles l'information a été initialement recueillie, et ce, sans le consentement de la personne ayant donné ces renseignements, ni compensation pour cette dernière. D'une part, la capacité d'accéder à des renseignements, de les restructurer et de les revendre peut être avantageuse pour les particuliers ainsi que les entreprises et créer des emplois. D'autre part, elle soulève des préoccupations, tant dans le grand public et dans le monde des affaires qu'au gouvernement, sur la protection de la vie privée et la sécurité des renseignements confidentiels.

Les sondages publics effectués auprès des Canadiens révèlent un souci prononcé de la protection de la vie privée. Le sondage effectué en 1992 par Ekos Research Associates Inc. sur le respect de la vie privée au Canada a permis de conclure que 92 p. 100 des 3 000 Canadiens interrogés considéraient la vie privée comme une question importante, et 60 p. 100 estimaient avoir perdu du terrain dans ce domaine, depuis une décennie. Les répondants ont aussi indiqué qu'ils seraient moins inquiets si les personnes utilisant leurs renseignements personnels exerçaient eux-mêmes un contrôle sur cette information, et s'ils savaient que leurs droits à la vie privée étaient protégés et que le gouvernement surveillait l'utilisation des renseignements. Selon une enquête faite en 1994 par Gallup Canada pour Andersen Consulting, plus de 80 p. 100 des Canadiens craignent que des renseignements personnels ne soient recueillis par des entreprises participant à l'autoroute de l'information. Ils croient que la vie privée est menacée de toute part, que ce soit par la technologie ou par les impératifs commerciaux et sociaux, et qu'il faut agir. Mais quel rôle devraient jouer le gouvernement, les entreprises et les particuliers ? De quelles préoccupations faut-il s'occuper ? Quelle est la solution ?

D'après la Constitution canadienne, la protection de la vie privée est un domaine de compétence partagé entre le gouvernement fédéral et les gouvernements provinciaux. En fait, les Canadiens ne sont que partiellement protégés par des lois fédérales et provinciales ainsi que par les codes volontaires établis par les administrations publiques et le monde des affaires. Ce document examine la pertinence du cadre législatif actuel du Canada en matière de protection de la vie privée ainsi que les récents efforts déployés par le gouvernement fédéral et les gouvernements provinciaux pour élargir et améliorer ce cadre afin de répondre aux nouvelles préoccupations.

Deux semaines après la date de clôture établie pour l'envoi des observations, toutes les présentations seront mises à la disposition du public, pendant les heures normales de bureau, à l'endroit suivant :

Bibliothèque d'Industrie Canada
2e étage, Tour Journal Sud
365 ouest, avenue Laurier
OTTAWA (Ont.)
K1A 0C8

et, pendant un an, dans les bureaux régionaux d'Industrie Canada à Halifax, à Montréal, à Toronto, à Edmonton et à Vancouver.

Préface

L'autoroute de l'information, une infrastructure complexe d'information et de communications, joue un rôle primordial dans la nouvelle économie informationnelle du Canada. Misant sur les réseaux actuels et prévus de télécommunications, cette infrastructure deviendra un « réseau de réseaux », liant foyers, entreprises, administrations publiques et organismes à une gamme étendue de services interactifs tels que loisirs, formation, culture, services sociaux, banques de données, ordinateurs, opérations bancaires et commerce électronique.

En mars 1994, le ministre de l'Industrie, John Manley, a constitué un comité consultatif national pour aider le gouvernement fédéral à élaborer et à mettre en œuvre une stratégie sur l'autoroute de l'information du Canada. Le Comité consultatif sur l'autoroute de l'information étudiera les questions soulevées dans le document de travail du gouvernement intitulé *L'autoroute canadienne de l'information : Une nouvelle infrastructure de l'information et des communications au Canada* (Ottawa, Approvisionnements et Services Canada, 1994), préparé par Industrie Canada, et proposera des solutions. Il examinera comment une infrastructure complexe d'information améliorera la croissance et la compétitivité des entreprises canadiennes; comment assurer à tous les Canadiens un accès universel et abordable aux services essentiels; comment établir un équilibre approprié entre la concurrence et la réglementation; comment promouvoir le développement ainsi que la diffusion de la culture et du contenu canadiens.

Le Comité a établi cinq groupes d'étude qui se penchent sur les grands domaines d'intérêt suivants : accès et incidences sociales; culture et contenu canadiens; compétitivité et création d'emplois; apprentissage et formation; recherche-développement : applications et développement du marché. Les groupes d'étude et le Comité se réunissent régulièrement et sont engagés dans diverses activités pour étudier les sujets en question, consulter le public et formuler des recommandations à l'intention du gouvernement fédéral.

Pour évaluer l'intérêt public et accroître la sensibilisation aux questions touchant la protection de la vie privée, Industrie Canada, en collaboration avec le Comité consultatif, a préparé ce document de travail intitulé *La protection de la vie privée et l'autoroute canadienne de l'information.* Industrie Canada publiera d'autres documents de travail sur des questions sociales, économiques et technologiques. Les personnes et les groupes intéressés sont invités à nous faire parvenir par écrit des présentations ou des observations sur les solutions proposées ou sur tout autre aspect du document de travail.

Les présentations doivent être adressées à :

Parke Davis, directeur général
Secrétariat du Comité consultatif
sur l'autoroute de l'information
Bureau 640
Tour Journal Nord
300, rue Slater
OTTAWA (Ont.)
K1A 0C8

Toutes les présentations doivent être reçues au plus tard le 23 décembre 1994 (se référer à la *Gazette du Canada,* Partie I).

Table des matières

La protection de la vie privée et l'autoroute canadienne de l'information ainsi que d'autres documents publiés par Industrie Canada sont disponibles sur le réseau informatique Internet en tapant council@istc.ca.

Les utilisateurs d'un protocole de transfert de fichier, de « Gopher » ou du réseau mondial (World Wide Web) peuvent avoir accès à ces ouvrages, en se servant des adresses suivantes d'Internet :

Protocole de transfert de fichier
debra.dgbt.doc.ca/pub/isc

Gopher
debra.dgbt.doc.ca port 70/Industry Canada Documents

Réseau mondial
http:/debra.dgbt.doc.ca/isc/isc.html

Pour obtenir des imprimés de ce document de travail, s'adresser à :

Service de distribution
Direction générale des communications
Industrie Canada
Bureau 208D, Tour est
235, rue Queen
OTTAWA (Ont.)
K1A 0H5
Téléphone : (613) 954-5716
Télécopieur : (613) 954-6436

Une publication complémentaire, *L'autoroute canadienne de l'information : Une nouvelle infrastructure de l'information et des communications au Canada,* est aussi disponible auprès de ce service.

Pour obtenir des renseignements sur le contenu de ce document de travail et sur le processus de consultation, s'adresser à :

Secrétariat du Comité consultatif
sur l'autoroute de l'information
Bureau 640
Tour Journal Nord
300, rue Slater
OTTAWA (Ont.)
K1A 0C8
Téléphone : (613) 990-4268
Télécopieur : (613) 941-1164.

N° au cat. C2-229/1-1994
ISBN 0-662-61370-8
SIT PU 0025-94-03

La protection de la vie privée et l'autoroute canadienne de l'information

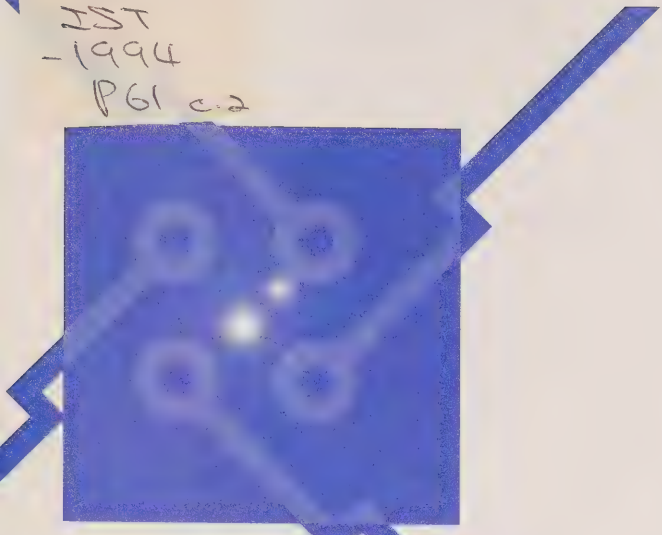
Direction générale du développement des communications
et de la planification
Secteur du spectre, des technologies de l'information
et des télécommunications
Industrie Canada
Octobre 1994

La protection de la vie privée et l'autoroute canadienne de l'information

Une nouvelle infrastructure de l'information et des communications au Canada

Industrie Canada Industry Canada

Canada



Privacy and the Canadian Information Highway

Building Canada's Information and Communications Infrastructure

Industry Canada Industrie Canada

Canada

Privacy and the Canadian Information Highway

Communications Development and Planning Branch
Spectrum, Information Technologies
and Telecommunications Sector
Industry Canada
October 1994

Privacy and the Canadian Information Highway and many other Industry Canada documents are available electronically on the Internet computer network at council@istc.ca.

Anyone with the ability to use Anonymous file transfer (FTP), Gopher or the World Wide Web can access these documents. Below are the Internet addresses:

Anonymous file transfer (FTP)
debra.dgbt.doc.ca/pub/isc

Gopher
debra.dgbt.doc.ca port 70/Industry Canada Documents

World Wide Web
http:/debra.dgbt.doc.ca/isc/isc.html

Additional print copies of this discussion paper are available from:

Distribution Services
Industry Canada
Room 208D, East Tower
235 Queen Street
OTTAWA, Ont
K1A 0H5
Tel.: (613) 954-5716
Fax: (613) 954-6436

A campanion document, *The Canadian Information Highway: Building Canada's Information and Communications Infrastructure,* is also available from this address.

For information about the contents of this discussion paper and the consultation process, contact:

Information Highway Advisory Council Secretariat
Room 640, Journal Tower North
300 Slater Street
OTTAWA, Ont.
K1A 0C8
Tel.: (613) 990-4268
Fax: (613) 941-1164

Cat. No. C2-229/1-1994
ISBN 0-662-61370-8
SIT PU 0025-94-03

Contents

Preface

The information highway of the future might be more accurately described as the advanced information and communications infrastructure that is essential for Canada's emerging information economy. Building on existing and planned communications networks, this infrastructure will become a "network of networks," linking Canadian homes, businesses, governments and institutions to a wide range of interactive services, from entertainment, educational and cultural products to social services, data banks, computers and electronic commerce as well as banking and business services.

Industry Minister John Manley in March 1994 created a national Information Highway Advisory Council to assist the federal government in developing and implementing a strategy for Canada's information highway. It is the council's responsibility to provide the necessary advice and guidance to government on the variety of issues raised in the government's discussion paper *The Canadian Information Highway: Building Canada's Information and Communications Infrastructure* (Ottawa: Minister of Supply and Services Canada, 1994), prepared by Industry Canada. Within this framework, the council will be examining how an advanced information infrastructure will improve the growth and competitiveness of Canadian businesses; how to ensure universal, affordable access to essential services for all Canadians; how to develop an appropriate balance between competition and regulation; and how to promote the development and distribution of Canadian culture and content.

Five working groups have been established by the advisory council to cover the following broad areas of interest: Access and Social Impact; Canadian Content and Culture; Competitiveness and Job Creation; Learning and Training; and R&D, Applications and Market Development. The working groups and the council meet on a regular basis and are engaged in a variety of activities to explore the issues, consult with the public and make recommendations to the federal government.

To seek the public's views and to raise the level of debate on privacy issues, Industry Canada is releasing the discussion paper *Privacy and the Canadian Information Highway* in cooperation with the advisory council. It is the first of several discussion documents to be released by Industry Canada on social, economic and technology policy issues. Written submissions and/or comments are invited from all interested parties on the various options and approaches presented or on any portion of this discussion paper.

Submissions should be addressed to:

Parke Davis, Director General
Information Highway Advisory
Council Secretariat
Room 640, Journal Tower North
300 Slater Street
OTTAWA, Ont.
K1A 0C8

All submissions must be received on or before December 23, 1994 (see *Canada Gazette,* Part I).

Two weeks after the closing date for comments, all submissions will be made available for viewing by the public, during normal business hours, at:

Industry Canada Library
2nd Floor, Journal Tower South
365 Laurier Avenue West
OTTAWA, Ont.
K1A 0C8

and at the regional offices of Industry Canada in Halifax, Montreal, Toronto, Edmonton and Vancouver for a period of one year.

Introduction

Businesses, public institutions and governments gather, store, transmit and exchange vast amounts of personal and business-related information both in paper format and electronically. The shift to computer-mediated interaction and the interconnection of networks will increase the amount of personal and transactional information that can be assembled into comprehensive profiles of individuals. In many cases, these records can be sent across national borders, sold or reused, or integrated with other data bases, for purposes unrelated to those for which the information was originally collected, without the consent of or compensation to the individual from whom the information was obtained. There is no question that the ability to access, repackage and resell information can benefit individuals and firms, and create new employment opportunities. On the other hand, it raises concerns among the general public, the business community and government alike about privacy protection and the security of sensitive information.

Public surveys of Canadians have consistently revealed a remarkably high level of concern over the issue of privacy. The 1992 Canadian Privacy Survey by Ekos Research Associates Inc. found that 92 percent of the 3 000 Canadians interviewed believed privacy to be an important issue, and that 60 percent believed they have less personal privacy now than a decade ago. Respondents also indicated they would be more at ease with others using their personal information if they had control over this information, knew their privacy rights were protected and knew government exercised some form of oversight or monitoring of these activities. A 1994 Gallup Canada survey for Andersen Consulting revealed that over 80 percent of the Canadians polled expressed concern about the personal information about them that might be collected by companies through the information highway. These studies suggest a pervasive belief that personal privacy is under siege from a range of technological, commercial and social threats and that something must be done about it. What is the role that government, businesses and individuals should play? What concerns must be addressed? What options are available?

Under the Canadian Constitution, the protection of privacy is a shared jurisdictional responsibility of the federal and provincial governments. In fact, Canadians are only partially protected by a combination of federal and provincial legislation, and voluntary codes set by government and the business community. The adequacy of Canada's current legislative framework for privacy protection is reviewed briefly in this paper, as are recent efforts, both federal and provincial, to broaden and enhance this framework to meet new privacy concerns.

In the "network of networks" world that is now emerging, Canada forms a part of the international "information grid" or "global village." As a sovereign nation, Canada has international commitments to a variety of treaties and conventions; as a trading nation and as a leader in communications technology and services, Canada has an interest in how other nations solve the privacy challenges facing us now. This paper also outlines Canada's participation in international organizations concerned with privacy protection and the efforts of some of our trading partners in this area. Finally, several approaches are proposed to strengthen personal privacy and data protection in Canada.

What Is Privacy?

Privacy is usually defined in two ways: the right to be left alone, free from intrusion or interruption, and the right to exercise control over one's personal information.

We Canadians value our right to live in peace, undisturbed by others. It is the right to solitude, to anonymity, to share our time with those we choose, and to define our own space and boundaries. This concept of privacy encompasses a broad range of issues that go beyond the acquisition and dissemination of personal information. While the *Canadian Charter of Rights and Freedoms* does not contain a specific right to privacy, it does guarantee an individual in his or her dealings with government the right to life, liberty and security of person, and the right to be secure from unreasonable search and seizure. Many privacy experts, however, would question the effectiveness of the protection available under the Charter.

Personal data protection has been defined as the claim of individuals to determine when, how and to what extent information about them is communicated to others. Data protection is an aspect of privacy protection that involves control over the collection, storage, accuracy, use and dissemination of personal information.

The high degree of mobility of modern Canadian lifestyles brings us into contact with a great many people who may not know us personally, except through various types of information we provide about ourselves. In travelling, shopping, obtaining services, driving our vehicles, and communicating from different locations, there is a need for us to provide secure identification of who we are and what we are entitled to receive. Service providers of all kinds require and ask for detailed information that will verify our identity and confirm our ability to pay. At the same time, these details and the data trails left by electronic transactions can be used to predict future marketing opportunities and thus increase the incentive to store this personal information in data bases. The exchange and marketing of personal information is flourishing, and it is increasingly taking place across national borders. As a result, data protection is becoming the most critical component of privacy protection.

Privacy Issues for the Information Highway

Transactional Data and Personal Profiling

Transactional data gathering will become much easier in a computer-mediated and networked world. The great strides in computing capacity, the linking of so many businesses by electronic payment systems, and the meshing of sales and ordering data bases have revolutionized the relationship between consumers and the producers of goods and services. With "just-in-time" supply management, producers manufacture and ship goods to warehouses and suppliers in direct response to the data transmitted from the point-of-sale terminals of their clients. Wholesalers and retailers increasingly are plugging into the chain. The linking of an individual to a particular purchase is merely one more segment of the chain, which facilitates direct marketing and market analysis. Most people may be aware that a credit card company could be selling their transactional data to vendors of products, but they might consider this a reasonable cost of doing business with a huge and reliable credit company, and one outweighed by the benefits. In the new networked environment, every business — large or small, reliable or not — will have the capacity to generate information files on its customers or to purchase customer data bases from other sources. What is the appropriate balance between the social and commercial benefits of such advanced technologies and the risks they bring to individual privacy? What controls or safeguards should be placed on the use and reuse of this information?

The information highway holds enormous potential to easily compile profiles of individuals' needs, lifestyle habits or purchase choices. This could have negative consequences if such profiles are used to deny opportunities to people without their knowledge. Data base storage and information cross-matching can be used to make decisions about individuals, affecting the terms and conditions of access to a variety of products, services and employment opportunities. This capability could further stigmatize the vulnerable — such as those who are ill, elderly or unemployed, or those who are seeking welfare, health care or citizenship — limiting their chances and curbing the gains we have made in equity and human rights in our society. In a highly competitive job market, where thousands of people send in résumés for

even modest jobs, what kinds of data base screening are we prepared to accept? How can unsuccessful job candidates ensure that they were not passed over because of erroneous information that appears on their records? Should organizations be required to notify individuals of their information holdings and provide no- or low-cost access to these files for verification or correction? Should there be time limits on the storage of information?

Provision of new services such as video on demand, and electronic magazines and catalogue services on the highway will permit the collection of an ever wider range of information regarding one's interests and choice of entertainment and reading material. Is some form of regulation needed to limit storage, access and use of such detailed data? Is it safe to permit such systems to gather information about our habits, even for benign purposes? How can individual privacy rights be protected during the different steps of the information collection, storage and exchange processes? Should informed consent be required for the different information activities and transactions an organization can undertake using personal information?

Transactional Security and Individual Identification

While encryption or encoding can secure the content of the electronic message, verifying the identities of the sender and the receiver is an equally critical element of privacy. This is especially true for financial and commercial information exchanges or for sending sensitive information. Increasingly, ordinary consumer transactions are not conducted in person, but through a variety of means, such as telephones, faxes or catalogue orders. Present methods of authentication and payment arrangements require various kinds of personal information that are not easily known by others, ranging from one's credit card number to the maiden name of one's mother. The extension of these commercial transactions at the consumer level to the terminal in the home poses new challenges. How can one verify a person's identity and/or credit worthiness for electronic orders or requests for delivery of medical records? Will present identification procedures continue to be adequate on the information highway? Would other methods, such as digital signatures, prove more secure?

Identity Cards and Single Identifier Numbers

Another aspect of the privacy debate is the issue of identity cards. New "smart card" technologies afford organizations the means of going beyond the limited information currently stored in magnetic strips to the enormous storage capacity of embedded chips. Detailed information or even pictures of the individual could be encoded on the card, or the data linked to a biometric identifier such as a thumbprint or retinal scan. With the current rates of fraud in card-based authorization systems — be they credit, phone or medical benefits cards — there is growing pressure to move to a more reliable system of identification. Privacy advocates, however, fear the potential of such cards to facilitate unacceptable levels of data matching, or the creation of a society in which it will be mandatory to carry identification documents on one's person at all times. In the face of strong public support for decreasing fraud in our social programs,

where is the line between responsible administration of programs and services, and unacceptable loss of individual liberties and privacy? A single numerical identifier increases the capability to amass and cross-match personal information. Should there be limits on such identifiers?

In the field of health information, privacy is a sensitive issue. Doctors, clinics and hospitals, insurers and governments, epidemiologists and researchers are motivated by differing interests with respect to health records, and may want access to lifelong data for legitimate purposes. But individuals, also legitimately, fear the abuse of this information by benefit providers or employers. In a Quebec trial use of a smart card for medical services, the information stored on the card was sequestered into four quadrants, with each service provider (such as a pharmacy) having access only to the information required. This solves one privacy problem because all players in the medical system are unable to access the complete range of patient data. However, the more fundamental issue of maintaining cradle-to-grave records through advances in technology remains a problem where privacy protection is not comprehensive.

Monitoring and Surveillance

Lifestyles, working patterns and business transactions will be transformed as computing and network power enter every home and business. While each information technology has different capabilities, they all contribute to an unprecedented capacity for surveillance of every man, woman and child, whether as customer, student, employee, patient, taxpayer or recipient of government services.

One of the most widely used applications on computer networks is electronic mail. The efficiency and convenience of this new information system have brought instant popularity in both commercial and social settings. Should employee e-mail be treated as a private letter, or as company property and therefore available to be read by a system operator or by a supervisor? Should these systems be designed to allow for easy encryption or encoding of the messages, to protect against casual forwarding and broadcasting of sensitive messages? Just as conventions and etiquette have been developed for the handling of personal and business correspondence over the centuries, should these norms be adapted to our new electronic environment?

Teleworking or working at home also brings a risk of increased surveillance. Managers may want to measure the productivity of employees who work at home by counting keystrokes, timing phone calls or wiring video cameras to the network. These techniques are already in use in some specialized areas of the work force. What limits, if any, need to be imposed on such monitoring? Is government regulation required, or will encouraging good behaviour and fair contracting practices suffice?

The information highway promises to support banking, teleworking, utility and appliance management, and other monitoring activities in the home. This raises serious questions not only about security of data on the network, but also about security in the home, whereby an intruder could enter and force the homeowner to withdraw money or to

credit another account through the home computer system. Home surveillance and protection systems offer security from burglary and fire, but how intimate should such systems be? Must there be a video data stream of every doorway and accessible window in our house sent to a security company or the police department? What controls should be put in place for the collection, use, availability and possible resale of information gathered about our use of different services in the home?

Another category of personal information is provided through satellite technology for global mobile telephone coverage. There will soon be available a unique individual telephone number that travels with each person, from the workplace to the home, the cottage, friends' apartments or businesses and other trips. Local cellular systems and other new personal communications services will have a similar capacity to track phones, using conventional radio and microwave technology. The gains in convenience are obvious, but the catch is that the computer must know exactly where each person is at all times. Privacy advocates want to know who will control the information about our whereabouts, how long it will be kept, and how far this "electronic leash" will extend. How should the different interests of employees and employers be balanced in this and similar forms of monitoring?

Intrusion

Citizens may also want to be protected from unwanted communications as a result of purchasing goods on the electronic highway. Disturbances or intrusions by telemarketers or targeted advertising mail is a privacy nuisance that concerns many Canadians. There is already "junk" fax, with solicitations over our fax machines for everything from coffee service to holiday trips. Should controls target marketing schemes that result from separate or related purchases — for instance, junk e-mail that follows a purchase of a Caribbean holiday with offers for a next trip? If so, how? What rules should govern the collection and use of information about what people buy or other personal information transactions? How should these rules be balanced with the opportunity to be made aware of goods or services that people might want and need?

What Privacy Protection Now Exists in Canada?

Over the past 20 years, the history of data protection legislation in the developed world has reflected the effort to balance what democratic countries perceive as the fundamental right of privacy and the need for government and business to obtain personal information that allows individuals to participate in a complex global society (see Annex A). Codes of fair information practices began to emerge, which limited the collection of information and established the right of the individual to access his or her own data, challenge its accuracy and correct any inaccuracies. During the 1970s, the Organisation for Economic Co-operation and Development (OECD) recognized the need to address the issue of personal privacy in the context of the growing transborder flow of information. Member countries, including Canada, started work on a set of guidelines. In 1981, the OECD released its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (see Annex B). Canada and other member countries adopted the Guidelines and indicated that they would be addressing privacy issues, either by passing legislation that incorporated the principles or by putting in place voluntary systems that would give force to them.

Protection in the Public Sector

Canada employs a mixture of legislation and voluntary codes to protect privacy. Data protection legislation protects personal information held by governments at the federal level and at some provincial and municipal levels. Based on the OECD Guidelines, the federal *Privacy Act* of 1982 protects information held by the federal government. The Office of the Privacy Commissioner was created to monitor the federal government's collection, use and disclosure of its clients' and employees' personal information, and its handling of individual requests to see personal records. In their annual reports to Parliament, Privacy Commissioners have not limited their comments to data protection within the federal government, but have reported on privacy trends across Canadian society. The cause of privacy protection has benefited greatly from these activities.

Some of the provinces have followed suit and have passed comprehensive legislation, starting with Quebec in 1982, Ontario in 1987, Saskatchewan in 1991, British Columbia in 1992 and Alberta in 1994. Nova Scotia introduced a privacy bill for the provincial public

sector in 1993. The powers of the various provincial commissioners or ombudsmen vary. For example, the British Columbia Commissioner can make binding orders, while the Ontario Commissioner makes recommendations. Only the Quebec Commissioner has jurisdiction over the private sector, with the power to impose fines for non-compliance of up to $20 000.

In Quebec, the issue of privacy has been addressed differently, partly because the Quebec *Civil Code* contains a specific and detailed right of privacy that covers private as well as public information holdings. Quebec has gone further than any other province by passing legislation that protects all personal information held by both the public and the private sectors. This legislation came into force in January 1994. It is one of the first data protection laws of its kind outside Europe, and has already had the effect of encouraging national operations to harmonize to the standard of data protection that must be met in Quebec.

Protection in the Private Sector

Apart from this effort in Quebec, the rapidly expanding use and management of personal information in the private sector is virtually unregulated in Canada, although there have been attempts in specific sectors to voluntarily set and implement fair information or privacy codes. These codes attempt to define boundaries and establish guidelines for personal privacy protection in order to achieve a balance between social and economic benefits, and an individual's right to control over his or her personal information.

The Canadian Direct Marketing Association, for example, has a voluntary code that offers consumers a chance to "opt out" or refuse to let their data be passed on or sold to other companies, and enjoins its members to make their best efforts to help consumers find out where erroneous information may have crept into their files.

The banking sector has had a privacy code since 1991, although the code and its implementation have fallen short of the expectations of privacy advocates, largely on the issues of client access to personal information and the amount of information required for granting credit. In public hearings in 1993, the Canadian Senate explored draft regulations that would address banking privacy concerns, should the Minister of Finance decide in the future that there is a need to regulate in this area. There has been no formal call, however, to move on this proposal.

The telecommunications sector has a mixture of a voluntary approach and regulation. The introduction of caller identification service, which displays the telephone number of the person calling, was criticized by a broad coalition of concerned citizens — from women's shelters to seniors' groups — for its inherent infringement on privacy. Telephone companies were eventually required by the Canadian Radio-television and Telecommunications Commission (CRTC) to offer free per-call blocking, and line blocking for those with particular needs. Around the same time, the privacy of cellular and mobile phones received widespread media attention after the private conversations of public figures were recorded using electronic scanners. In response to these

and other concerns, such as the proliferation of telemarketing and junk fax, the federal government announced a set of Telecommunications Privacy Principles (see Annex C) in December 1992. These principles were designed to encourage awareness of privacy concerns within the industry and to promote a self-regulatory approach. They reinforced the rights of individuals to control their personal information and to be made aware of the privacy implications of new communications and information technology products and services. Although the Telecommunications Privacy Protection Agency, which was proposed to oversee the implementation of these principles, has never materialized into an active force, the principles have influenced the development of voluntary codes within the telecommunications sector.

The new *Telecommunications Act,* which came into effect in October 1993, provides the CRTC with enhanced powers to protect the privacy of individuals and to regulate unsolicited communications. The government also introduced amendments to the *Criminal Code* and the *Radiocommunication Act,* which came into effect in August 1993, forbidding the divulgence of intercepted radio-based telephone communications.

In addition to these sector-specific initiatives, Canada is experimenting with a more inclusive national model code. In the fall of 1990, the Canadian Standards Association (CSA) initiated the development of a national privacy standard that could be applied across all sectors and all provinces. Several federal departments, key private sector players and various consumer representatives are participating in this initiative, and a draft code is expected to be available for public comment late in 1994. With a standards-based approach to data protection, privacy could be addressed during the development of new information and communications technologies, and could be promoted with our trading partners internationally. A national standard for data protection developed in Canada could be included as an element in the International Organization for Standardization's quality management standards (ISO 9000 series), increasing the likelihood that large corporations would treat the management of personal data in the same way they do security, clean room facility management and other quality control mechanisms.

How Have Other Countries Protected Privacy?

The European approach to privacy favours omnibus data protection regulations that apply to both the public and private sectors, and are overseen by independent data commissioners. Countries whose histories have made them sensitive to data protection issues, such as Germany, France, Austria and Sweden, passed laws in the 1970s and, by the end of that decade, there was sufficient imbalance of protection in Europe that the Council of Europe began to discuss a Convention that would bind member countries to producing similar legislation. The OECD developed its Guidelines in 1981 in order to provide the same kind of harmonization among its member states, fearing that the disparity in protection of privacy rights would cause countries with data protection to block the flows of data to those without it. By the end of the 1980s, many European countries had still failed to produce data protection legislation, even though they were obliged by Convention 108 of the Council of Europe. The Commission of the European Community, concerned that data commissioners might block data transfers between countries and thus hinder the development of a single European common market, decided to act.

In 1990, the Commission of the European Community released two draft data protection directives, which, if passed by the European Parliament, will have the force of law. The first was a general directive applying to all personal data, computerized or in manual files, which banned data flows to countries without adequate protection. The second was a tightly modelled directive on privacy in telecommunications, which dictated the precise response member countries and trading partners should take to the intrusions posed by caller identification, cellular and speaker phones, and call detail recording. Response to this initiative was swift, with many businesses and member countries opposed to various aspects of the directive. In 1992, the main directive reappeared with greatly reduced extraterritoriality, and a later version is expected to be passed by the end of 1994.

In contrast, the United States has tended to rely on voluntary codes of practice and sectoral legislation. In 1970, the U.S. passed the first *Fair Credit Reporting Act*, recognizing that the detailed profiling necessary for credit activities must be balanced by opportunities for consumers to examine

their files and correct errors. The federal *Privacy Act* was passed in 1974 to protect the privacy of individuals with respect to information contained in federal government records that was likely to be released under the new *Freedom of Information Act* (FOIA). However, the emphasis was clearly on the FOIA, and there was no independent oversight of the *Privacy Act*. In response to scandals in the credit business, the United States is revising its fair credit reporting legislation.

The United States is also taking a fresh look at privacy in the context of its National Information Infrastructure (NII) initiative, which is similar to Canada's efforts to seek advice on what the future information highway should be. It has struck a task force to look solely at privacy issues. The Working Group on Privacy of the NII Task Force has tabled privacy principles for comment, but the oversight mechanisms are as yet unspecified. The National Telecommunications and Information Agency, the arm of the Commerce Department responsible for policy advice on the NII, has issued a call for comment on the implications for privacy of new telecommunications services, with a discussion paper exploring some of the issues in transaction-generated information.

Possible Approaches for Canada

Most Canadians doubt their ability to protect their privacy, and see the role of protection as a government responsibility or a joint government/business partnership. Undoubtedly, the development of the information highway will continue to raise these issues and the demand for action.

Possible approaches to privacy protection include legislation, the advancement of a national voluntary privacy standard, the promotion of privacy protective technologies such as encryption and smart cards, and consumer education. Canada may need all of these approaches.

Legislation and Regulation

Protection of the enormous information holdings of governments, including medical, welfare, tax, immigration and police records, exists at the federal level and in the provinces of Quebec, Ontario, Saskatchewan, Alberta and British Columbia. The quality of coverage varies from jurisdiction to jurisdiction and, when information travels, it is not always clear which law applies. Reflecting this environment in its 1993–94 annual report, the Office of the Privacy Commissioner described Canada's privacy protection as a patchwork of public and private initiatives that address privacy in a piecemeal fashion. The commissioner called for "national privacy legislation to establish the principles and framework" for both business and government. There is no doubt that both provincial commissioners and governments have recognized these problems too, and it may be time to initiate a dialogue to work toward solutions.

Although federal legislation may well be desirable to provide uniform protection and rights across Canada, the division of authority between federal and provincial jurisdictions appears to preclude this from happening. The federal government has the power to regulate industries such as telecommunications, transportation carriers and banks. The provinces, however, have responsibility for privacy protection in areas such as individual transactions between consumers and the retail industry. By amending existing sectoral legislation, the federal government could create privacy protection requirements in each sector it regulates. Another possible approach would be to extend the federal *Privacy Act* to all sectors of the marketplace within federal jurisdiction. Since this might further exacerbate disparities between regulated and non-regulated entities, it would make sense for jurisdictions to work together toward a common set of rules that could be applied in all sectors.

Federal legislation would respond to the expressed desire of Canadians for a government oversight role in consumer protection. It could also serve to initiate a dialogue for improved privacy protection at the provincial and territorial level. A complementary federal and provincial framework could address such shared concerns as the potential for interprovincial trade barriers caused by differing privacy protection requirements and practices among provinces and territories. It would have to address the need for a level playing field between competing businesses and for consumers coast to coast. The private sector currently faces different regulatory regimes. For example, the privacy protection clauses of the *Telecommunications Act* apply to federally regulated carriers, but not to telecommunications resellers and information service providers. The cost of meeting differing standards is passed on to consumers in the prices of goods and services.

Many segments of the population would favour a legislative approach. The 1992 Canadian Privacy Survey found that a clear majority of Canadians favoured government legislation or a government/private sector partnership to develop privacy protection guidelines for the private sector. A 1992 Equifax Canada study of Consumers and Privacy in the Information Age found that 84 percent of the insurance, financial and credit bureau executives surveyed believed that federal legislation is required to set rules for the collection and circulation of consumer information, thereby avoiding a patchwork of disparate provincial regimes. While this appears to go against today's trend toward a deregulatory environment and reduction of government, it may in fact recognize that harmonized basic rules for data protection are good for business and may be possible without excessive bureaucracy. Setting ground rules enables all players to compete fairly, and establishes consumer confidence.

Voluntary Codes and Standards

Voluntary codes have been the preferred approach of Canadian business and industry associations. This approach allows for flexibility in application, so that different industries can tailor their data protection schemes to the needs of their customers, the regulatory environment in which they operate and the demands of the marketplace.

There is no need for voluntary codes to be any less stringent than those enforced by law, but it is this very matter of enforceability that is giving consumer advocates grounds for concern. Who is ultimately accountable? To whom does an aggrieved consumer go for redress? As the value of personal information increases with the growth of the information economy, how can voluntary codes unsanctioned by law ensure its protection? Past experience with voluntary codes has not been encouraging because they frequently do not meet the 1981 OECD Guidelines. As a result, they are considered by most privacy experts as inadequate to cope with the privacy threats of the 1990s.

The CSA's project to develop a national privacy standard extends the voluntary code approach. By setting out the basic principles that must be addressed in a code, the standard strengthens the often weak and ambiguous language used in codes. Oversight in the form of auditing and certification by a standards

body, such as the Quality Management Institute, a division of the CSA, could provide a level of protection similar to that in a legislated regime. Successful privacy protection by means of the proposed CSA voluntary standard, however, will be difficult if it is not adopted fully and implemented broadly by industry associations and companies.

Contractual approaches also have been suggested, whereby consumers would agree to the use of their data for specific purposes, perhaps in return for discounts or fees. Care must be taken that such a market-driven approach does not result in privacy for only the rich. At present, few individuals understand the market value of their personal information or know how to protect it. In addition, contracts that limit or waive fundamental privacy values have the potential to become an industry practice in the absence of clearly defined privacy rights.

Technological Solutions

Another approach to privacy protection is to use technology to safeguard personal data. Traditionally, technology has been exploited to increase the amount of information gathered, and hence has been feared rather than welcomed by privacy activists. But technology itself is neutral, and can be used to enhance privacy as well as threaten it. Technologies can be designed so that the "default setting" is on zero information collection. Telephone systems can be designed to "forget" the last few digits of a telephone number after placing a call, in order to protect privacy in personal billing statements. Electronic mail systems can be developed that provide ephemeral messages for personal use, a sort of electronic disappearing ink. Should the design for the information highway explicitly enhance the ability of the individual to control his or her personal and transactional information?

An important yet underexplored territory is encryption or encoding. Strong encryption is now available and can be incorporated into software, embedded as chips in equipment such as telephone sets or palm-sized computers, or used in smart cards. Smart cards, through the use of public key encryption, can provide fraud-proof guarantees of identity or credentials, and yet allow the holder to be completely anonymous. The same technology can be used to provide reliable but virtually untraceable electronic cash — a far safer method for the consumer than releasing a charge card number over the information highway.

Technologies brought to market can have profound effects on the rights of consumers, but how can consumers affect the technology development process? Should there be public hearings, such as the CRTC has for telecommunications services when a new technology is brought to market? Should the privacy implications of all new information systems and standards be explored in public fora? Is it a responsibility of government, or should it be up to the marketplace to determine what levels of privacy protection will be offered? Should privacy be an optional extra, for which only some Canadians can afford to pay, or should privacy be cost-neutral and considered an essential part of service offerings?

Consumer Education

There is a fundamental need to educate businesses about the need for more enlightened approaches to the handling of personal data, and to raise the awareness of consumers about how to protect themselves. Consumers need information and education about their rights, about the value of their personal information, about the risks to their privacy that new technologies can bring, and about what they can do to retain privacy. Although most Canadians see the role of protecting privacy as a government responsibility or perhaps a partnership of government and business, they also feel that the individual has a strong role to play in solving privacy problems. What should be the relative balance of responsibilities?

Public Comment

The intent of this paper is to contribute to the debate on the social and economic impact of the information highway, not to offer definitive solutions. Comments from individuals, organizations and institutions in both the private and public sectors are welcome. Written submissions and/or comments on the approaches to privacy protection are invited on the following questions, or on any portion of this discussion paper. They should be sent to the address mentioned in the Preface.

- What principles should form the basis of effective privacy protection?
- Does government need to introduce stronger measures to protect the privacy and security of information? How can each of the four approaches described above be used effectively?
- Is a national level of privacy protection needed, or can adequate privacy protection on the information highway be provided through provincial or sectoral legislation?
- In which circumstances might voluntary privacy guidelines developed by businesses be appropriate?
- Should the information highway be designed to provide high levels of privacy protection, or will this slow the pace and raise the cost of innovation?
- How can Canadians become better involved in the design process for potentially privacy-threatening technologies and services?
- How can Canadians become better informed about the value of their personal information and the need for controlling its use? What role should businesses and governments play in educating the public?

Annexes

A — Chronology of Background Events

The issue of privacy in an information-based economy arose globally in the 1970s. In Canada, the former Department of Communications joined with the Department of Justice in forming the Task Force on Privacy and Computers, which issued a report titled *Privacy and Computers* (Ottawa: Information Canada, 1972) and several studies. At the OECD, privacy was addressed as an issue of transborder data flows. Member countries realized that they had a common interest in protecting privacy and individual liberties, and in reconciling the fundamental but competing values of privacy and the free flow of information. It was recognized that transborder flows of personal data contribute to economic and social development, and that restrictions on these flows could interfere with the operations of multinational enterprises and cause serious disruptions in important economic sectors such as banking, insurance and travel. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were promulgated. At about the same time, the Council of Europe passed a similar document, Convention 108, to which European countries varied greatly in their legislative responses. It was the sluggishness on the part of member states to take action that prompted the European Community to introduce much stiffer Community directives with the force of law.

Key events and players are listed below in chronological order:

1969 OECD recognizes privacy implications of transborder data flow; Group of Experts struck in 1978

1970 U.S. *Fair Credit Reporting Act*

1972 Report of the joint Justice–Communications task force on privacy and computers

1977 Privacy Commissioner established under *Canadian Human Rights Act*

1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

1981 Interdepartmental Task Force on Transborder Data Flows struck in Canada

1982 Council of Europe passes Convention 108 on data protection; Canada passes *Privacy Act* for federally held records

1984 Canada signs OECD Guidelines; Department of Justice responsible for urging compliance of industry

1987 Report of Standing Committee on Justice reviewing *Privacy Act* implementation criticizes lack of compliance with OECD Guidelines in private sector and government inertia

1990 European Community tables draft directives on data protection and data protection in telecommunications; U.S. and international players mount vigorous lobby to water down transborder data flows and trade-restrictive aspects of directive

1991 OECD revisits data protection; European Community seeks to protect its privacy directives in the General Agreement on Tariffs and Trade; key federal departments back CSA's bid to develop a model OECD-based code of practice, along with industry and consumer groups

1992 Department of Communications tables Telecommunications Privacy Principles and drafts legislation on cellular privacy

1993 Federal government passes new *Telecommunications Act,* which came into effect October 25, 1993, giving CRTC a specific mandate with respect to the protection of privacy in telecommunications and substantial powers to exercise this mandate; Quebec passes Bill 68, law on protection of personal information in the private sector, which came into effect January 1, 1994

B — The OECD Guidelines and the Draft CSA Privacy Standard

Drafted at the end of the 1970s and adopted as a recommendation of the Council of the OECD in September 1980, the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data provided a sound basis for fair information practices at the time, and constituted a remarkable document for a group of countries largely without data protection laws. Nevertheless, the Guidelines may require some further specifications in the context of the technologies of the 21st century. The main concepts are as follows:

- Eight basic principles of national application are set out in Part Two of the Guidelines, covering data Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation and Accountability.
- Four principles of international application covering Free Flow and Legitimate Restrictions are set out in Part Three of the Guidelines.

When the CSA went about drafting its model privacy code, it used the OECD Guidelines as a starting point, interpreting them afresh in the Canadian context of 1991. It is important to evaluate the CSA standard in its entirety, since the commentary on the principles is important to the understanding of each principle. However, because the draft is not yet available for public discussion, its 10 principles are listed below only briefly, with a note where there is deviation from the OECD Guidelines. Public comment on the final draft will be invited in the fall of 1994.

1. Accountability (seen to be so fundamental that it must be the first principle)
2. Identifying purposes
3. Consent (new)
4. Limiting collection
5. Limiting use, disclosure, retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance (new; gives individual the right to challenge an organization's compliance with any of the principles, not just the accuracy of the individual's data)

C — *Telecommunications Privacy Principles*

- Canadians value their privacy. Personal privacy considerations must be addressed explicitly in the provision, use and regulation of telecommunications services.
- Canadians need to know the implications of the use of telecommunications services for their personal privacy. All providers of telecommunications services and government have a responsibility to communicate this information in an understandable and accessible form.
- When telecommunications services that compromise personal privacy are introduced, appropriate measures must be taken to maintain the consumers' privacy at no extra cost unless there are compelling reasons for not doing so.
- It is fundamental to privacy that there be limits to the collection, use and disclosure of personal information obtained by service providers and generated by telecommunications networks. Except where clearly in the public interest, or as authorized by law, such information should be collected, used and disclosed only with the express and informed consent of the persons involved.
- Fundamental to privacy is the right to be left alone. A balance should exist between the legitimate use of unsolicited telecommunications and their potential for intrusion into personal privacy. All parties have a responsibility to establish ground rules and methods of redress so that Canadians are able to protect themselves from unwanted and intrusive telecommunications.
- Privacy expectations of Canadians may change over time. Methods of protecting telecommunications privacy must be reviewed from time to time to meet these changing expectations and to respond to changing technologies and services.

C — *Principes de protection de la vie privée dans les télécommunications*

- Les Canadiens accordent une grande importance à leur vie privée. Les facteurs relatifs aux renseignements personnels doivent être exposés explicitement dans les documents sur la prestation, l'utilisation et la réglementation des services de télécommunications.
- Les Canadiens doivent connaître les répercussions de l'utilisation des services de télécommunications sur leur vie privée. Il incombe à tous les fournisseurs de services de télécommunications ainsi qu'à l'administration publique de communiquer ces renseignements, de manière compréhensible et accessible.
- Lorsqu'on introduit des services de télécommunications qui font intrusion dans la vie privée, il faut prendre des mesures appropriées pour protéger la vie privée du consommateur sans frais supplémentaires, sauf dans des cas exceptionnels.
- Il est indispensable pour la vie privée qu'il y ait des limites à la collecte, à l'utilisation et à la divulgation de renseignements personnels obtenus par les fournisseurs de services et de produits par les réseaux de télécommunications. Sauf dans les cas qui sont clairement dans l'intérêt public, ou en cas d'autorisation par la loi, ces renseignements ne doivent être recueillis, employés et divulgués qu'avec le consentement explicite et éclairé des personnes visées.
- L'un des principes de base de la vie privée est le droit d'être laissé seul. Il faut instaurer un équilibre entre l'usage légitime des télécommunications non sollicitées et leur potentiel d'intrusion dans la vie privée personnelle. Toutes les parties en cause doivent établir des règles de base ainsi que des méthodes de compensation afin que les Canadiens puissent se protéger contre les télécommunications indésirables et intrusives.
- Les attentes des Canadiens en ce qui concerne leur vie privée peuvent changer avec le temps. Les méthodes de protection de la vie privée en matière de télécommunications doivent être révisées de temps à autre en fonction de ces nouvelles attentes ainsi que de l'évolution de la technologie et des services.

B — Les lignes directrices de l'OCDE et le projet de l'Association canadienne de normalisation sur l'élaboration d'une norme sur la protection de la vie privée

Établies à la fin des années 70 et adoptées sous forme d'une recommandation du Conseil de l'OCDE en septembre 1980, les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel ont constitué une base de saines pratiques d'information à l'époque, et représentent une réalisation remarquable pour un groupe de pays largement dépourvus de lois sur la protection des données. Néanmoins, les Lignes directrices exigeront peut-être d'autres précisions dans le cadre de la technologie du XXI[e] siècle. Les concepts visés se retrouvent dans les principes ci-dessous :

- Huit principes fondamentaux applicables sur le plan national sont exposés à la Partie deux des Lignes directrices. Ils portent sur la limitation en matière de collecte, la qualité des données, la précision des finalités, la limitation de l'utilisation, les garanties de sécurité, la transparence, la participation et la responsabilité individuelles.
- Quatre principes applicables sur le plan international, portant sur la libre circulation et les restrictions légitimes, sont exposés à la Partie trois des Lignes directrices.

Lorsque l'Association canadienne de normalisation a élaboré son code modèle sur la vie privée, elle s'est inspirée des Lignes directrices de l'OCDE, les interprétant dans le contexte canadien de 1991. Il est important d'évaluer la norme de l'Association dans son entier, étant donné que le commentaire sur les principes est important pour la compréhension de chacun de ces derniers. Cependant, étant donné que le projet n'est pas encore soumis à l'examen public, les 10 principes ne sont que brièvement exposés ci-après, accompagnés d'une explication lorsqu'ils sont différents des Lignes directrices de l'OCDE. Le public sera invité à commenter la version finale, à l'automne de 1994.

1. Responsabilité (considérée comme fondamentale au point d'être le premier principe)
2. Énoncé des finalités
3. Consentement (nouveau)
4. Limitation en matière de collecte
5. Limitation de l'usage, de la divulgation ou de la conservation
6. Exactitude
7. Garanties
8. Transparence
9. Accès individuel
10. Refus de conformité (nouveau; donne au particulier le droit de contester la conformité d'un organisme à l'un ou à l'autre des principes, et non seulement l'exactitude des données touchant le particulier).

1987 Le Comité permanent de la justice présente son rapport examinant l'application de la *Loi sur la protection des renseignements personnels* et critiquant l'absence de conformité du secteur privé aux Lignes directrices de l'OCDE ainsi que l'inertie gouvernementale.

1990 La Communauté européenne présente des projets de directives sur la protection des données en général ainsi qu'en matière de télécommunications; les États-Unis et des intervenants de l'étranger entament des démarches dynamiques pour diminuer l'importance des aspects de la directive sur les flux transfrontières de données et pour diminuer les aspects restrictifs pour le commerce.

1991 L'OCDE remanie le concept de protection des données; la Communauté européenne cherche à protéger ses directives sur la vie privée dans l'Accord général sur les tarifs douaniers et le commerce.

1991 Les principaux ministères fédéraux, de même que l'industrie et des groupes de consommateurs, appuient la demande présentée par l'Association canadienne de normalisation pour élaborer un code de pratique modèle fondé sur l'OCDE.

1992 Le ministère des Communications présente les *Principes de protection de la vie privée dans les télécommunications,* et rédige un projet de loi sur la protection des communications par téléphones cellulaires.

1993 La nouvelle *Loi sur les télécommunications* est adoptée par le gouvernement fédéral et entre en vigueur le 25 octobre 1993; elle donne au CRTC un mandat précis visant à protéger la vie privée dans les télécommunications, et lui confère des pouvoirs étendus à cette fin.

1993 Le Québec adopte le projet de loi 68 sur la protection des renseignements personnels dans le secteur privé, qui est devenu loi le 1er janvier 1994.

Annexes

A — Chronologie des activités

La question de la vie privée dans une économie fondée sur l'information s'est posée à l'échelle mondiale dans les années 70. Au Canada, l'ancien ministère des Communications s'est joint au ministère de la Justice pour former un groupe d'études sur les ordinateurs et la vie privée, groupe qui a préparé plusieurs études, notamment un rapport intitulé *Les ordinateurs et la vie privée* (Ottawa, Information Canada, 1972). L'OCDE, pour sa part, considérait la protection de la vie privée comme touchant les flux transfrontières de données, et les pays membres ont constaté qu'ils avaient mutuellement intérêt à protéger la vie privée et les libertés individuelles ainsi qu'à concilier les valeurs fondamentales mais concurrentielles de la vie privée et de la libre circulation de l'information. On a reconnu que les flux transfrontières de données à caractère personnel contribuent au développement socio-économique et que des restrictions en la matière pourraient nuire aux activités de multinationales et perturber gravement des secteurs économiques importants comme les banques, les assurances et les voyages. L'OCDE a promulgué les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel. Vers la même époque, le Conseil de l'Europe adoptait un document similaire, la Convention 108, auquel les pays européens ont réagi de façon très différente sur le plan législatif. C'est la lenteur des membres à intervenir qui a incité la Communauté européenne à introduire des directives plus strictes ayant force de loi.

Voici les principaux événements et intervenants, dans l'ordre chronologique :

1969 L'OCDE reconnaît les répercussions des flux transfrontières de données sur la vie privée; un groupe de spécialistes est constitué en 1978.

1970 Les États-Unis adoptent le *Fair Credit Reporting Act.*

1972 Le groupe d'études Justice-Communications présente son rapport sur les ordinateurs et la vie privée.

1977 Le poste de Commissaire à la protection de la vie privée est établi en vertu de la *Loi canadienne sur les droits de la personne.*

1980 L'OCDE promulgue les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel.

1981 Un groupe de travail interministériel sur les flux transfrontières de données est créé au Canada.

1982 Le Conseil de l'Europe adopte la Convention 108 sur la protection des données; le Canada adopte la *Loi sur la protection des renseignements personnels,* pour les dossiers relevant de l'administration fédérale.

1984 Le Canada signe les Lignes directrices de l'OCDE; le ministère de la Justice est chargé d'inciter l'industrie à se conformer rapidement à ce document.

6 Commentaires publics

Ce document vise à contribuer au débat sur les répercussions socio-économiques de l'autoroute de l'information, et non à proposer des solutions définitives. Les particuliers et les organismes publics et privés sont invités à nous faire part de leurs vues. Ils sont priés de faire parvenir par écrit leurs commentaires sur les démarches en la matière, les questions suivantes ou tout autre aspect du présent document de travail. Se référer à l'adresse indiquée dans la préface.

- Quels principes devraient être à la base d'une protection efficace de la vie privée ?
- Le gouvernement doit-il introduire des mesures plus fermes pour protéger la vie privée et la sécurité de l'information ? Comment peut-on utiliser efficacement chacune des quatre démarches décrites ci-dessus ?
- Faut-il instaurer une protection à l'échelle nationale ou au contraire faire confiance à une réglementation provinciale ou sectorielle ?
- Dans quelles circonstances conviendrait-il de recourir à des lignes directrices volontaires sur la vie privée préparées par le monde des affaires ?
- L'autoroute de l'information devrait-elle être conçue pour assurer un niveau élevé de protection ou, au contraire, une telle structure ralentirait-elle le rythme et ferait-elle augmenter le coût de l'innovation ?
- Comment les Canadiens peuvent-ils participer davantage au processus de conception de techniques et de services susceptibles de menacer la vie privée ?
- Comment les Canadiens peuvent-ils se renseigner davantage sur la valeur de leurs renseignements personnels et sur la nécessité d'en contrôler l'utilisation ? Quel rôle le monde des affaires et les pouvoirs publics doivent-ils jouer dans l'éducation du public ?

La technologie établie sur le marché peut avoir de grandes répercussions sur les droits des consommateurs, mais comment ceux-ci peuvent-ils modifier le processus de mise au point technologique ? Devrait-il y avoir des audiences publiques, comme celles du CRTC pour les services de télécommunications, lorsqu'une nouvelle technologie arrive sur le marché ? Faudrait-il examiner au moyen de tribunes publiques les conséquences de tous les nouveaux systèmes et normes d'information sur la vie privée ? Incombe-t-il au gouvernement ou au marché de déterminer les niveaux de protection à offrir ? La vie privée devrait-elle être une option, que seuls certains Canadiens pourraient se permettre, ou n'entraîner aucun coût et être considérée comme inhérente aux services offerts ?

Éducation des consommateurs

Il est essentiel de sensibiliser le monde des affaires à la nécessité d'aborder de façon plus éclairée la manutention des données personnelles, et de sensibiliser les consommateurs aux façons de se protéger. Les consommateurs ont besoin de renseignements et d'éducation sur leurs droits, la valeur de leurs renseignements personnels, les risques présentés par la nouvelle technologie à leur vie privée et les mesures qu'ils peuvent prendre pour préserver cette dernière. Bien que la plupart des Canadiens considèrent la protection de la vie privée comme une responsabilité gouvernementale, voire celle d'un partenariat entre les pouvoirs publics et les entreprises, ils estiment que le particulier a un grand rôle à jouer pour résoudre les problèmes dans ce domaine. Comment les responsabilités devraient-elles être partagées ?

sanctions légales ? L'expérience avec des codes volontaires n'a pas été jusqu'ici encourageante, ceux-ci n'étant pas toujours conformes aux Lignes directrices de 1981 de l'OCDE. Selon la plupart des spécialistes en matière de vie privée, ces codes sont insuffisants pour parer aux risques des années 90.

Le projet de l'Association canadienne de normalisation sur l'élaboration d'une norme nationale sur la vie privée dépasse le cadre des codes volontaires. En définissant les principes de base de tout code, la norme apporte une solution au langage souvent faible et ambigu utilisé dans la rédaction des codes. Une protection similaire à celle d'une législation pourrait être assurée au moyen d'une vérification et d'une certification faites par un organisme de normalisation tel que le Quality Management Institute, une division de l'Association canadienne de normalisation. Il sera difficile de protéger efficacement la vie privée au moyen de la norme volontaire proposée par l'Association, si cette norme n'est pas adoptée entièrement et mise en œuvre dans toutes les associations industrielles et les entreprises.

On a aussi proposé des démarches contractuelles, selon lesquelles les consommateurs accepteraient que leurs données soient utilisées à des fins précises, peut-être en retour d'escomptes ou d'honoraires. Il faut veiller à ce qu'une telle démarche axée sur le marché ne réserve pas la protection de la vie privée aux riches. Actuellement, peu de gens comprennent la valeur marchande de leurs renseignements personnels ou savent comment les protéger. En outre, les contrats qui limitent ou suppriment les valeurs fondamentales de la vie privée sont susceptibles de devenir une pratique industrielle en l'absence de droits clairement définis.

Solutions technologiques

Une autre démarche consiste à utiliser la technologie pour protéger les données personnelles. Traditionnellement, la technologie a plutôt servi à augmenter le nombre des renseignements recueillis, de sorte que les partisans actifs de la vie privée ont plutôt tendance à s'en méfier. Cependant, la technologie en soi est neutre et peut servir à améliorer la vie privée autant qu'à la menacer. Il est possible de concevoir des techniques de manière que le réglage implicite corresponde à une absence de collecte de données. De même, des systèmes téléphoniques peuvent « oublier » les derniers chiffres d'un numéro de téléphone après un appel, afin de protéger la vie privée dans les énoncés de facturation personnelle. Des systèmes de courrier électronique peuvent fournir des messages éphémères pour usage personnel, au moyen d'une encre électronique qui s'estompe. La conception de l'autoroute de l'information devrait-elle améliorer la capacité d'une personne de contrôler ses renseignements personnels ainsi que transactionnels ?

Un domaine aussi important que mal étudié est le codage ou le chiffrement. Un codage fort peut maintenant être intégré à des logiciels, à des puces dans un équipement comme des postes téléphoniques ou de minuscules ordinateurs, ou encore être utilisé dans des cartes intelligentes. Ces dernières, grâce à un chiffrement à clé révélée, peuvent protéger l'identité ou les titres contre toute fraude, et permettre au détenteur de rester anonyme. La même technologie peut servir à se procurer des fonds d'une manière électronique et fiable, mais pratiquement impossible à retracer, ce qui est une méthode beaucoup plus sûre pour le consommateur que la diffusion d'un numéro de carte de crédit sur l'autoroute de l'information.

secteurs du marché placés sous juridiction fédérale. Comme cette démarche pourrait aggraver les disparités entre les entités réglementées et celles non réglementées, il faudrait collaborer avec d'autres autorités pour établir un ensemble de règles communes à tous les secteurs.

Une loi fédérale répondrait au désir exprimé par les Canadiens de voir instaurer une supervision gouvernementale de la protection des consommateurs. Elle pourrait aussi servir à amorcer un dialogue pour améliorer la protection de la vie privée aux niveaux provincial et territorial. Un cadre fédéral et un cadre provincial complémentaires réduiraient les préoccupations communes, dont la possibilité de barrières commerciales interprovinciales causées par des exigences ainsi que des pratiques en matière de protection de la vie privée variant d'une province ou d'un territoire à l'autre. La loi devrait permettre d'uniformiser les règles du jeu entre les entreprises concurrentielles et les consommateurs, et ce, d'un océan à l'autre. Le secteur privé est actuellement assujetti à divers régimes de réglementation. Ainsi, les clauses de protection de la vie privée contenues dans la *Loi sur les télécommunications* s'appliquent aux entreprises assujetties à une réglementation fédérale, mais non aux revendeurs de télécommunications ni aux fournisseurs de services d'information. Étant intégré dans le prix des biens et des services, le coût de la disparité des normes est assumé par les consommateurs.

De nombreux segments de la population favoriseraient une démarche législative. Le sondage canadien de 1992 sur le respect de la vie privée démontrait qu'une grande majorité de Canadiens était en faveur d'une législation gouvernementale ou d'un partenariat entre le secteur public et le secteur privé pour élaborer des lignes directrices à l'intention du secteur privé. Selon le rapport Equifax Canada sur les consommateurs et la vie privée à l'ère de l'information, publié en 1992, 84 p. 100 des cadres des compagnies d'assurances, des services financiers et des bureaux de crédit croient qu'une législation fédérale est nécessaire pour fixer des règles présidant à la collecte et à la circulation des renseignements sur les consommateurs et éviter ainsi un ensemble disparate de régimes provinciaux. Cette vue semble aller à l'encontre de la tendance actuelle vers la déréglementation et la réduction du contrôle gouvernemental, mais elle reconnaît peut-être que des règles de base harmonisées pour la protection des données profitent au commerce et peuvent être appliquées sans trop de bureaucratie. En effet, ces règles permettraient à tous les intervenants de soutenir la concurrence de manière équitable et susciteraient la confiance chez les consommateurs.

Codes et normes volontaires

Permettant aux diverses industries d'adapter leurs dispositifs de protection des données aux besoins de leurs clients, au milieu de réglementation où elles opèrent ainsi qu'aux exigences du marché, les codes volontaires sont la méthode préférée des gens d'affaires et des associations industrielles du Canada.

Il n'est pas nécessaire que les codes volontaires soient moins stricts que ceux imposés par la loi, mais c'est la question même du caractère exécutoire qui préoccupe les défenseurs des consommateurs. Qui est responsable en fin de compte ? A qui un consommateur lésé doit-il s'adresser pour obtenir réparation ? Étant donné que la valeur des renseignements personnels augmente en fonction d'une économie de plus en plus axée sur l'information, comment assurer la protection de ces renseignements sans l'aide de

5 Les démarches possibles pour le Canada

La plupart des Canadiens doutent de leur capacité de protéger leur vie privée, et croient que cette responsabilité incombe aux pouvoirs publics ou à un partenariat entre le secteur public et le monde des affaires. La mise au point de l'autoroute de l'information encouragera sûrement le débat sur ces questions et les demandes d'intervention.

Parmi les démarches possibles pour protéger la vie privée, notons les lois, une norme nationale et volontaire améliorée sur la vie privée, la promotion de techniques comme le codage et les cartes intelligentes ainsi que l'éducation des consommateurs. Le Canada devra peut-être recourir à toutes ces solutions.

Lois et réglementation

L'énorme réserve de renseignements détenus par les autorités (dossiers médicaux et fiscaux, dossiers d'assistance sociale, d'immigration et de police), est protégée à un certain point au niveau fédéral et au Québec, en Ontario, en Saskatchewan, en Colombie-Britannique et en Alberta. La qualité de la protection varie d'un secteur de compétence à l'autre; de plus, lorsque l'information se déplace, on ne sait pas toujours par quelle loi elle est régie. Constatant cette situation dans son rapport de 1993-1994, le Commissariat à la protection de la vie privée décrivait la protection au Canada comme une mosaïque d'initiatives publiques et privées qui abordent le sujet de façon disparate. Le commissaire prônait l'adoption d'une loi nationale sur la protection de la vie privée pour établir les principes et le cadre de cette protection, à la fois pour le monde des affaires et pour le secteur public. Les commissaires provinciaux et les gouvernements ayant eux aussi reconnu ces problèmes, il est peut-être temps d'entamer un dialogue pour trouver des solutions.

Bien qu'une loi fédérale soit souhaitable pour assurer une protection et des droits uniformes dans tout le Canada, la séparation des pouvoirs entre les secteurs de compétence fédéraux et provinciaux est un obstacle. Le gouvernement fédéral a le pouvoir nécessaire pour réglementer des industries comme les télécommunications, les transporteurs et les banques. Toutefois, les provinces exercent des responsabilités dans les transactions individuelles entre consommateurs et le commerce au détail. En modifiant les lois sectorielles actuelles, le gouvernement fédéral pourrait créer des exigences en matière de protection de la vie privée dans chaque secteur réglementé. Une autre option serait d'appliquer la *Loi sur la protection des renseignements personnels* à tous les

d'examiner leurs fichiers et de corriger les erreurs. En 1974, la loi fédérale *Privacy Act* était adoptée pour protéger la vie privée des particuliers en ce qui concerne les renseignements contenus dans les registres de l'administration fédérale et susceptibles d'être divulgués en vertu du nouveau *Freedom of Information Act.* On insistait cependant sur cette dernière et l'on ne prévoyait aucune surveillance indépendante de l'application de la *Privacy Act.* Pour parer aux scandales dans le monde du crédit, les États-Unis révisent actuellement leurs lois sur les rapports équitables en matière de crédit.

Ce pays réexaminent aussi la protection de la vie privée dans le contexte de l'initiative National Information Infrastructure (NII), se rapprochant des démarches du Canada pour demander des conseils sur la nature souhaitable de la future autoroute de l'information. Les États-Unis ont constitué un groupe de travail chargé d'examiner uniquement les questions relatives à la vie privée. Ce groupe a présenté des principes aux fins de commentaires, mais n'a pas encore prévu de mécanismes de supervision. La National Telecommunications and Information Agency, service du Department of Commerce chargé des conseils sur les politiques relatives à la NII, a lancé un appel pour recueillir des commentaires sur les conséquences des services de télécommunications sur la vie privée, et a publié un document de travail traitant de questions touchant les renseignements relatifs aux transactions.

La protection de la vie privée dans d'autres pays

L'Europe privilégie des règlements généraux sur la protection des données, applicables aux secteurs public et privé, et supervisés par des commissaires indépendants chargés des données. Les pays dont l'histoire les a sensibilisé aux questions de protection des données (Allemagne, France, Autriche, Suède) ont adopté des lois au cours des années 70. A la fin de cette décennie, il existait sur ce continent un tel déséquilibre dans ce domaine que le Conseil de l'Europe amorça des pourparlers sur une convention qui obligerait les pays membres à adopter des lois similaires. En 1981, l'OCDE élaborait ses Lignes directrices pour assurer le même type d'harmonisation parmi ses États membres, craignant que la disparité dans la protection des droits de la vie privée n'incite les pays protégeant les données à bloquer le flux de ces dernières vers les nations plus laxistes. A la fin des années 80, bon nombre de pays européens n'avaient toujours pas émis de lois sur la protection des données même s'ils y étaient obligés par la Convention 108 du Conseil de l'Europe. La Commission des Communautés européennes, inquiète à l'idée que les commissaires chargés des données pouvaient bloquer des transferts entre les pays et ainsi nuire au développement d'un marché européen commun, passa à l'action.

En 1990, elle publiait deux projets de directives sur la protection des données qui, si elles sont adoptées par le Parlement européen, auront force de loi. La première, une directive générale sur toutes les données personnelles, informatisées ou manuelles, interdisait le flux de données vers les pays dépourvus d'une protection adéquate. La deuxième, très structurée, portait sur la vie privée en matière de télécommunications et dictait les mesures précises que devraient prendre les pays membres ainsi que les partenaires commerciaux contre les intrusions suscitées par l'identification des appelants, les téléphones cellulaires et à haut-parleur ainsi que l'enregistrement des données d'appels. Bon nombre d'entreprises et de pays membres se sont vite opposés à divers aspects de la directive. En 1992, la principale directive réapparaissait avec une extraterritorialité largement réduite; une version ultérieure sera sans doute adoptée d'ici la fin de 1994.

Les États-Unis, pour leur part, ont tendance à se fonder sur des codes de pratique volontaires et des lois sectorielles. En 1970, ils adoptaient le premier *Fair Credit Reporting Act*, reconnaissant que les profils détaillés nécessaires aux activités de crédit devaient être compensés par la possibilité, pour les consommateurs,

prolifération du télémarketing et de la publicité importune par télécopieur, le gouvernement fédéral a annoncé, en décembre 1992, des principes de protection de la vie privée dans les télécommunications (voir annexe C). Ces principes visaient à sensibiliser l'industrie aux préoccupations sur la vie privée ainsi qu'à promouvoir une démarche fondée sur l'autoréglementation. Ils renforcent les droits des particuliers à contrôler leurs renseignements personnels et à se renseigner sur les répercussions que peuvent avoir, sur leur vie privée, les nouveaux produits et services de communications ainsi que d'information. Bien que le projet d'agence de protection de la vie privée en matière de télécommunications, proposé pour superviser la mise en œuvre de ces principes, ne se soit jamais concrétisé, les principes ont influé sur l'élaboration de codes volontaires dans le secteur des télécommunications.

La nouvelle *Loi sur les télécommunications*, entrée en vigueur en octobre 1993, donne au CRTC des pouvoirs accrus pour protéger la vie privée des particuliers et réglementer les communications non sollicitées. Le gouvernement a aussi introduit des modifications au Code criminel ainsi qu'à la *Loi sur la radiocommunication*, entrés en vigueur en août 1993 et interdisant la divulgation des communications téléphoniques radio interceptées.

En plus de ces initiatives sectorielles, le Canada fait l'essai d'un code type national plus complet. A l'automne 1990, l'Association canadienne de normalisation a commencé à élaborer une norme nationale sur la vie privée, qui pourrait s'appliquer à tous les secteurs et à toutes les provinces. Plusieurs ministères fédéraux, des intervenants clés du secteur privé et divers représentants des consommateurs participent à cette initiative. Un projet devrait être présenté au public à la fin de 1994. Une démarche normalisée de la protection des données pourrait permettre d'examiner la question de la vie privée pendant la mise au point de techniques d'information et de communications, et l'on pourrait en faire la promotion auprès des partenaires commerciaux à l'étranger. Une norme élaborée au Canada pourrait être incluse dans les normes de gestion de la qualité de l'Association internationale de normalisation (série ISO 9000) pour inciter les grandes entreprises à traiter la gestion des données personnelles de la même façon que la sécurité, la gestion des salles blanches et d'autres mécanismes de contrôle de la qualité.

Les pouvoirs des commissaires ou des ombudsmans provinciaux varient. Ainsi, le commissaire de la Colombie-Britannique peut émettre des arrêts exécutoires, tandis que celui de l'Ontario formule des recommandations. Seul celui du Québec exerce une juridiction sur le secteur privé, auquel il peut imposer, en cas de dérogation, des amendes allant jusqu'à 20 000 $.

Au Québec, la question de la vie privée a été examinée différemment, surtout parce que le Code civil prévoit un droit spécifique et détaillé à la vie privée, lequel englobe les renseignements privés aussi bien que publics. Le Québec est allé plus loin que toutes les autres provinces en adoptant une loi protégeant tous les renseignements personnels détenus tant par le secteur public que par le secteur privé. Entrée en vigueur en janvier 1994, cette loi est l'une des premières du genre à être appliquée hors de l'Europe et a déjà incité les organismes nationaux à se fonder sur les mêmes normes.

La protection dans le secteur privé

Hormis cette initiative au Québec, l'utilisation croissante des renseignements personnels et leur gestion dans le secteur privé sont très peu réglementés au Canada. Certains secteurs ont pourtant volontairement tenté d'établir et de mettre en œuvre des codes équitables sur l'information ou la vie privée. Ces codes tentent de définir les limites et d'établir des lignes directrices pour la protection des renseignements personnels afin d'instaurer un équilibre entre les avantages socio-économiques et le droit d'une personne de contrôler les renseignements qui la concernent.

L'Association canadienne du marketing direct a un code volontaire qui offre aux consommateurs la possibilité de déroger au processus ou de refuser que leurs données soient transmises ou vendues à d'autres entreprises. Elle enjoint ses membres d'aider les consommateurs à déceler les informations erronées qui se seraient glissées dans leurs dossiers.

Depuis 1991, le secteur des opérations bancaires dispose d'un code sur la vie privée. Son contenu et son application n'ont cependant pas été conformes aux attentes des défenseurs de la vie privée, surtout pour ce qui est de l'accès du client aux renseignements personnels et du nombre de renseignements requis pour accorder un crédit. Dans des audiences publiques tenues en 1993, le Sénat canadien a étudié un projet de règlement qui porterait sur les préoccupations des banques dans le cas où le ministre des Finances réglementerait ce secteur. Il n'y a toutefois eu aucun appel officiel pour concrétiser cette proposition.

Le secteur des télécommunications présente un mélange de méthodes volontaires et de réglementation. L'introduction de services d'identification de l'appelant, soit l'affichage du numéro de téléphone de ce dernier, a été critiquée par une forte coalition de citoyens inquiets — depuis les responsables de refuges pour femmes jusqu'aux foyers pour personnes âgées — pour son intrusion inhérente dans la vie privée. Le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) a obligé les compagnies de téléphone à offrir gratuitement un blocage par appel et un blocage de ligne aux personnes ayant des besoins spéciaux. Les médias se sont aussi largement intéressés au caractère privé des conversations par téléphones cellulaires et mobiles après que des entretiens privés de personnalités publiques aient été enregistrés au moyen d'appareils de balayage électronique. En réponse à ces préoccupations ainsi qu'à la

3 La protection de la vie privée au Canada

Depuis 20 ans, la législation sur la protection des données dans les pays industrialisés reflète les efforts déployés pour établir un équilibre entre, d'une part, ce que les pays démocratiques considèrent comme le droit fondamental à la vie privée et, d'autre part, la nécessité pour les pouvoirs publics et les entreprises d'obtenir des renseignements personnels permettant aux particuliers de participer à une société universelle complexe (voir annexe A). Des codes sur les pratiques équitables en matière d'information limitent la collecte de renseignements et donnent au particulier le droit d'accéder aux données qui le concernent, d'en contester l'exactitude et de corriger les erreurs, le cas échéant. Au cours des années 70, l'Organisation de coopération et de développement économiques (OCDE) a reconnu la nécessité d'examiner la question de la vie privée dans le contexte du flux croissant de données transfrontières. Les pays membres, dont le Canada, ont commencé à élaborer des lignes directrices. En 1981, l'OCDE a diffusé ses Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel (voir annexe B). Le Canada et d'autres pays membres ont adopté ces lignes directrices et ont indiqué qu'ils aborderaient les questions relatives à la vie privée, soit en adoptant des lois intégrant les principes en question, soit en instaurant des systèmes volontaires permettant de leur donner du poids.

La protection dans le secteur public

Le Canada emploie un ensemble de lois et de codes volontaires pour protéger la vie privée, applicables notamment aux renseignements personnels détenus par le gouvernement fédéral, certains gouvernements provinciaux et certaines municipalités. Fondée sur les Lignes directrices de l'OCDE, la *Loi sur la protection des renseignements personnels,* de 1982, protège l'information détenue par le gouvernement fédéral. Le Commissariat à la protection de la vie privée a été créé pour surveiller la façon dont le gouvernement fédéral recueille, utilise et divulgue les renseignements personnels sur ses clients et ses employés, et sur la façon dont il traite les demandes de consultation de dossiers personnels. Dans les rapports annuels au Parlement, les commissaires à la protection de la vie privée n'ont pas limité leurs commentaires à la protection des données au sein du gouvernement fédéral, mais ont examiné les tendances qui existent dans toute la société canadienne. Ces activités ont grandement servi la cause de la protection de la vie privée.

Certaines provinces ont emboîté le pas et ont adopté des lois exhaustives : le Québec, en 1982, l'Ontario, en 1987, la Saskatchewan, en 1991, la Colombie-Britannique, en 1992, l'Alberta, en 1994. La Nouvelle-Écosse a présenté en 1993 un projet de loi sur la protection de la vie privée pour le secteur public provincial.

Le télétravail ou travail à domicile présente aussi un risque de surveillance accrue. Les gestionnaires désireront peut-être mesurer la productivité des employés qui travaillent à domicile, en comptant les frappes de clavier, en mesurant la durée des appels téléphoniques ou en branchant des caméras vidéo au réseau. Ces techniques sont déjà utilisées dans certains secteurs de travail spécialisés. Quelles limites, si besoin est, faut-il imposer à une telle surveillance ? Une réglementation gouvernementale s'imposera-t-elle, ou suffira-t-il d'encourager un bon comportement et de justes pratiques contractuelles ?

L'autoroute de l'information promet de favoriser les opérations bancaires, le télétravail, la gestion des services publics et des appareils électroménagers ainsi que des activités de surveillance au foyer. Cela soulève de graves questions, non seulement sur la sécurité des données comprises dans le réseau, mais aussi sur la sécurité dans un logement, où un intrus pourrait pénétrer et forcer le propriétaire, par le biais de son ordinateur, à retirer de l'argent ou à créditer des fonds à un autre compte. Les systèmes de surveillance et de protection de domiciles offrent une garantie contre les voleurs et les incendies, mais dans quelle mesure doit-on leur confier des renseignements personnels ? Faut-il accepter qu'un flux de données vidéo sur chaque entrée et fenêtre de son domicile soit transmis à une compagnie de sécurité ou au service de police ? Comment contrôler la collecte, l'usage, la disponibilité, voire la revente de l'information recueillie sur l'utilisation des différents services à domicile ?

La technologie des satellites applicable aux téléphones mobiles dans le monde entier fournit une autre catégorie de renseignements personnels. Bientôt un numéro de téléphone unique et individuel se déplacera avec chacun, du lieu de travail au domicile, au chalet, à l'appartement d'un ami ou en voyage. Grâce à une technologie conventionnelle de radio et à hyperfréquences, des systèmes cellulaires locaux et d'autres services de communications personnelles permettront de retracer les conversations téléphoniques. Bien que très commode, cette situation signifie que l'ordinateur devra toujours savoir exactement où se trouve la personne. Les défenseurs du droit à la vie privée voudront savoir qui contrôlera l'information sur les allées et venues, pendant combien de temps cette information sera conservée et jusqu'où s'étendra cette laisse électronique. Dans une telle forme de surveillance et dans le cadre de méthodes semblables, comment établir un équilibre entre les intérêts des employés et ceux des employeurs ?

Intrusion

Les citoyens souhaiteront aussi être protégés contre les communications indésirables à la suite d'un achat fait par l'intermédiaire de l'autoroute de l'information. Les intrusions par les télévendeurs ou par le courrier publicitaire ciblé dérangent bon nombre de Canadiens. Déjà, des sollicitations importunes par télécopieur sont reçues pour tout genre de services, de la vente de café aux voyages d'agrément. Faut-il contrôler les programmes de commercialisation ciblés qui découlent d'achats séparés ou connexes (par exemple, les sollicitations envoyées par courrier électronique après l'achat d'un voyage dans les Caraïbes et qui proposent d'autres voyages) ? Dans l'affirmative, comment ? Quelles règles devraient régir la collecte et l'utilisation de l'information sur nos achats ou sur d'autres transactions personnelles ? Comment instaurer un équilibre entre ces règles et les possibilités d'être renseignés sur les biens ou services voulus ?

pourraient être codés sur la carte, ou encore les données pourraient être liées à un identificateur biométrique comme l'empreinte du pouce ou l'empreinte rétinienne. Étant donné le nombre actuel de fraudes commises au moyen de systèmes d'autorisation par cartes — qu'il s'agisse de cartes de crédit, de cartes d'appel ou de cartes santé — une pression de plus en plus forte s'exerce en faveur d'un système d'identification plus fiable. Les défenseurs du droit à la vie privée craignent toutefois que ces cartes ne facilitent un couplage inacceptable des données, ou la création d'une société où il serait obligatoire de porter en tout temps des documents d'identité sur soi. Le public souhaitant vivement une diminution des fraudes qui grèvent nos programmes sociaux, où se trouve l'équilibre entre, d'une part, une administration responsable des programmes et services et, d'autre part, une érosion inacceptable des libertés individuelles et du droit à la vie privée ? Un numéro identificateur unique accroît la capacité de recueillir et d'assortir des renseignements personnels. Devrait-il y avoir des limites à ces identificateurs ?

Dans le domaine de l'information sur la santé, la vie privée est une question délicate. Les médecins, les cliniques et les hôpitaux, les assureurs et les pouvoirs publics, les épidémiologistes et les chercheurs s'intéressent aux besoins médicaux pour des motifs différents, et pourraient vouloir accéder à des données sur la vie d'une personne pour des raisons très valables. Cependant, les particuliers, tout aussi légitimement, craignent que les fournisseurs d'avantages ou les employeurs n'abusent de cette information. Sur une carte santé intelligente mise à l'essai au Québec, les renseignements ont été stockés sur quatre quadrants; chaque fournisseur de service (par exemple, une pharmacie) n'avait accès qu'à l'information qui le concernait. Cette solution résout le problème que pose l'accès de tous les intervenants dans le système médical à la gamme complète de données, mais ne règle pas la question fondamentale posée par une technologie qui favorise la création de fichiers de la naissance à la mort et l'intrusion dans la vie privée que cela signifie.

Surveillance et contrôle

Les styles de vie, les régimes de travail et les transactions commerciales seront transformés à mesure que le pouvoir de l'informatique et des réseaux pénétrera dans chaque domicile et entreprise. Bien que chacune des techniques de l'information présente des caractéristiques différentes, elles contribuent toutes à établir une capacité sans précédent de surveillance de chaque homme, femme et enfant, qu'il s'agisse d'un client, d'un étudiant, d'un employé, d'un patient, d'un contribuable ou d'un bénéficiaire de services gouvernementaux.

L'une des applications les plus communes des réseaux informatiques est le courrier électronique. L'efficience et la commodité de ce nouveau système d'information lui ont valu une popularité instantanée dans les secteurs tant commerciaux que sociaux. Le courrier électronique d'un employé devrait-il être traité comme une lettre privée ou au contraire comme un bien appartenant à une entreprise et, par conséquent, susceptible d'être lu par un opérateur de système ou par un superviseur ? Ces systèmes devraient-ils être conçus pour faciliter le codage ou le chiffrement des messages, pour les protéger contre l'envoi et la diffusion par inadvertance de messages confidentiels ? Tout comme ont été élaborées des conventions et une étiquette pour la manipulation du courrier personnel et d'affaires à travers les siècles, faudrait-il adapter ces normes au nouveau milieu électronique ?

des soins médicaux, ou la citoyenneté canadienne), limitant leurs chances et annulant les progrès de la société en matière d'équité et de droits de la personne. Sur un marché du travail très concurrentiel, où des milliers de personnes envoient des curriculum vitæ même pour de modestes emplois, quel genre de présélection à partir de bases de données sommes-nous disposés à accepter ? Comment les postulants non retenus pourront-ils s'assurer que leur candidature n'a pas été rejetée à cause d'une information erronée qui figurait dans leur fichier ? Les organismes devraient-ils être tenus de communiquer aux particuliers les renseignements détenus à leur sujet, et de leur fournir, à peu de frais ou gratuitement, un accès à ces fichiers aux fins de vérification ou de correction ? Devrait-on imposer des limites de temps au stockage de l'information ?

La prestation de nouveaux services par l'intermédiaire de l'autoroute de l'information, tels la vidéo sur demande, les magazines et les catalogues électroniques, permettra de recueillir des renseignements encore plus variés sur les intérêts et les choix de certaines personnes en matière de divertissement et de lectures. Faut-il établir une réglementation pour limiter le stockage et l'utilisation de ces données détaillées, ainsi que l'accès à celles-ci ? Y a-t-il un danger à permettre à ces systèmes de recueillir des renseignements sur nos habitudes, même à des fins anodines ? Comment peut-on protéger les droits individuels à la vie privée pendant les différentes étapes de la collecte, du stockage et de l'échange de l'information ? Devrait-on exiger un consentement donné en toute connaissance de cause pour les différentes activités et transactions en matière d'information qu'un organisme peut entreprendre en utilisant des renseignements personnels ?

Sécurité transactionnelle et identification individuelle

Bien que l'on puisse protéger le contenu d'un message électronique par codage ou chiffrement, la vérification de l'identité d'un expéditeur et d'un destinataire constitue un élément critique de la protection de la vie privée, notamment pour les échanges de renseignements financiers et commerciaux ou pour l'envoi de renseignements confidentiels. Les transactions ordinaires se font de moins en moins souvent en personne, mais plutôt au moyen du téléphone, du télécopieur ou de commandes par catalogues. Les méthodes actuelles d'authentification et de paiement exigent divers types de renseignements personnels qui ne sont pas facilement connus, depuis le numéro de carte de crédit jusqu'au nom de jeune fille de la mère d'une personne donnée. La possibilité, pour les consommateurs, d'effectuer des transactions commerciales par voie électronique à partir de leur domicile pose de nouveaux défis. Comment vérifier l'identité ou la solvabilité d'une personne qui passe une commande électronique ou demande la livraison de dossiers médicaux ? Est-ce que les méthodes actuelles d'authentification suffiront sur l'autoroute de l'information ? D'autres méthodes, telles les signatures numériques, seraient-elles plus sûres ?

Cartes d'identité et numéros identificateurs uniques

Un autre aspect du débat sur la vie privée est l'émission de cartes d'identité. La nouvelle technologie relative aux cartes intelligentes donne aux organismes les moyens de dépasser les capacités actuelles de stockage sur les bandes magnétiques, pour accéder à l'énorme potentiel de stockage des puces intégrées. Des renseignements détaillés sur une personne, voire des photos,

2 Les effets de l'autoroute de l'information sur la vie privée

Données transactionnelles et profils personnels

La collecte de données transactionnelles deviendra beaucoup plus facile dans un monde informatisé et maillé. Les grands progrès réalisés quant à la capacité des ordinateurs, la liaison d'un grand nombre d'entreprises par des systèmes de paiement électronique, et le maillage complet des bases de données sur les ventes et les commandes ont révolutionné la relation entre les consommateurs et les producteurs de biens et de services. Grâce à la gestion de l'approvisionnement « juste-à-temps », les producteurs fabriquent et expédient les biens aux entrepôts et aux fournisseurs selon l'information reçue des terminaux situés aux points de vente de leurs clients. Les grossistes et les détaillants se raccordent de plus en plus à cette chaîne. Le lien entre une personne et un achat particulier n'est qu'un maillon de plus de la chaîne, qui facilite la commercialisation directe et l'analyse de marché. La plupart des gens savent qu'un établissement émetteur de cartes de crédit peut vendre les données transactionnelles qui les concernent à des fournisseurs de produits, mais ils peuvent considérer ce risque comme un inconvénient raisonnable compensé par l'avantage du recours à un établissement de crédit important et fiable. Dans le nouveau milieu maillé, toutes les entreprises, grandes ou petites, fiables ou non, seront en mesure de constituer des fichiers de données sur leur clientèle ou d'acheter des bases de données sur les clients auprès d'autres fournisseurs. Quel est le meilleur équilibre entre les avantages sociaux et commerciaux d'une technologie aussi avancée et les dangers qu'elle représente pour la protection de la vie privée ? Quels contrôles et quelles mesures de protection faut-il imposer quant à l'utilisation et à la réutilisation de cette information ?

L'autoroute de l'information pourrait grandement faciliter l'établissement du profil des personnes en fonction de leurs besoins, de leur style de vie ou de leurs choix d'achats. Cela pourrait avoir des répercussions malencontreuses si ces profils servaient à empêcher les personnes, et ce, à leur insu, de saisir les occasions qui s'offrent à elles. Le stockage dans des bases de données et les rapprochements des renseignements permettraient de prendre des décisions sur des particuliers, ce qui modifierait les conditions d'accès à divers produits, services et perspectives d'emploi. Cette situation pourrait pénaliser les personnes déjà vulnérables (malades, personnes âgées ou chômeurs, celles qui cherchent à obtenir des prestations d'aide sociale,

Qu'est-ce que la vie privée ?

La vie privée est normalement définie de deux façons : le droit de vivre en paix, sans intrusion ni interruption, et le droit de contrôler les renseignements qui touchent sa personne.

Les Canadiens accordent une grande importance au droit de vivre en paix, sans être dérangés. C'est le droit à la solitude, à l'anonymat, au partage de son temps avec des personnes choisies, ainsi que le droit de définir son espace et ses frontières. Ce concept englobe plusieurs questions qui dépassent l'acquisition et la diffusion de renseignements personnels. Bien que la *Charte canadienne des droits et libertés* ne contienne aucun droit spécifique en matière de vie privée, elle garantit à une personne, dans ses rapports avec le gouvernement, le droit à la vie, à la liberté et à la sécurité personnelles ainsi que le droit à la protection contre une fouille et une saisie déraisonnables. Bon nombre de spécialistes doutent cependant de l'efficacité de la protection offerte par la Charte.

Par protection des données personnelles, on entend la revendication, par des personnes, du droit de déterminer quand, comment et dans quelle mesure des renseignements qui les concernent sont communiqués à autrui. La protection des données est un aspect de la protection de la vie privée qui comprend le contrôle exercé sur la collecte, le stockage, l'exactitude, l'utilisation et la diffusion de renseignements personnels.

La grande mobilité dont jouissent les Canadiens les amènent à être connus de diverses personnes non pas personnellement, mais par le biais des informations disponibles à leur sujet. Quand nous voyageons, effectuons des emplettes, obtenons des services, conduisons un véhicule ou communiquons à partir de différents emplacements, notre identité et nos droits doivent être bien définis. Les fournisseurs de services de tous genres demandent des renseignements détaillés permettant de vérifier notre identité et de confirmer notre capacité de payer. Simultanément, ces renseignements et les données laissées par les transactions électroniques permettent de prévoir les possibilités de commercialisation, et donc incitent les personnes à conserver ces renseignements personnels dans des banques de données. L'échange et la commercialisation de renseignements personnels sont de plus en plus répandus dans le monde. La protection des données devient donc l'élément clé de la protection de la vie privée.

Dans le « réseau de réseaux », le Canada forme un maillon de la « chaîne d'information » internationale ou du « village planétaire ». A titre de nation souveraine, il a pris des engagements à l'échelle internationale, dans le cadre de divers traités et conventions; à titre de nation commerciale et de chef de file en technologie et en télécommunications, le Canada s'intéresse à la façon dont d'autres pays réagissent face aux défis que suscite la protection de la vie privée. Ce document traite aussi de la participation canadienne à des organismes internationaux soucieux de protéger la vie privée, ainsi que des efforts déployés par certains des partenaires commerciaux du Canada dans ce domaine. Enfin, diverses méthodes sont proposées pour étendre la protection des données et de la vie privée au Canada.

Introduction

Les entreprises, les organismes publics et les administrations publiques rassemblent, stockent, transmettent et échangent un grand nombre de renseignements personnels et professionnels, sous forme imprimée ou électronique. Le passage à l'interaction informatisée et l'interconnexion de réseaux augmentent le nombre de renseignements pouvant former le profil d'un individu. Ces données peuvent être envoyées à l'étranger, vendues ou réutilisées; elles peuvent être intégrées à des bases de données autres que celles pour lesquelles l'information a été initialement recueillie, et ce, sans le consentement de la personne ayant donné ces renseignements, ni compensation pour cette dernière. D'une part, la capacité d'accéder à des renseignements, de les restructurer et de les revendre peut être avantageuse pour les particuliers ainsi que les entreprises et créer des emplois. D'autre part, elle soulève des préoccupations, tant dans le grand public et dans le monde des affaires qu'au gouvernement, sur la protection de la vie privée et la sécurité des renseignements confidentiels.

Les sondages publics effectués auprès des Canadiens révèlent un souci prononcé de la protection de la vie privée. Le sondage effectué en 1992 par Ekos Research Associates Inc. sur le respect de la vie privée au Canada a permis de conclure que 92 p. 100 des 3 000 Canadiens interrogés considéraient la vie privée comme une question importante, et 60 p. 100 estimaient avoir perdu du terrain dans ce domaine, depuis une décennie. Les répondants ont aussi indiqué qu'ils seraient moins inquiets si les personnes utilisant leurs renseignements personnels exerçaient eux-mêmes un contrôle sur cette information, et s'ils savaient que leurs droits à la vie privée étaient protégés et que le gouvernement surveillait l'utilisation des renseignements. Selon une enquête faite en 1994 par Gallup Canada pour Andersen Consulting, plus de 80 p. 100 des Canadiens craignent que des renseignements personnels ne soient recueillis par des entreprises participant à l'autoroute de l'information. Ils croient que la vie privée est menacée de toute part, que ce soit par la technologie ou par les impératifs commerciaux et sociaux, et qu'il faut agir. Mais quel rôle devraient jouer le gouvernement, les entreprises et les particuliers ? De quelles préoccupations faut-il s'occuper ? Quelle est la solution ?

D'après la Constitution canadienne, la protection de la vie privée est un domaine de compétence partagé entre le gouvernement fédéral et les gouvernements provinciaux. En fait, les Canadiens ne sont que partiellement protégés par des lois fédérales et provinciales ainsi que par les codes volontaires établis par les administrations publiques et le monde des affaires. Ce document examine la pertinence du cadre législatif actuel du Canada en matière de protection de la vie privée ainsi que les récents efforts déployés par le gouvernement fédéral et les gouvernements provinciaux pour élargir et améliorer ce cadre afin de répondre aux nouvelles préoccupations.

Deux semaines après la date de clôture établie pour l'envoi des observations, toutes les présentations seront mises à la disposition du public, pendant les heures normales de bureau, à l'endroit suivant :

Bibliothèque d'Industrie Canada
2e étage, Tour Journal Sud
365 ouest, avenue Laurier
OTTAWA (Ont.)
K1A 0C8

et, pendant un an, dans les bureaux régionaux d'Industrie Canada à Halifax, à Montréal, à Toronto, à Edmonton et à Vancouver.

Préface

L'autoroute de l'information, une infrastructure complexe d'information et de communications, joue un rôle primordial dans la nouvelle économie informationnelle du Canada. Misant sur les réseaux actuels et prévus de télécommunications, cette infrastructure deviendra un « réseau de réseaux », liant foyers, entreprises, administrations publiques et organismes à une gamme étendue de services interactifs tels que loisirs, formation, culture, services sociaux, banques de données, ordinateurs, opérations bancaires et commerce électronique.

En mars 1994, le ministre de l'Industrie, John Manley, a constitué un comité consultatif national pour aider le gouvernement fédéral à élaborer et à mettre en œuvre une stratégie sur l'autoroute de l'information du Canada. Le Comité consultatif sur l'autoroute de l'information étudiera les questions soulevées dans le document de travail du gouvernement intitulé *L'autoroute canadienne de l'information : Une nouvelle infrastructure de l'information et des communications au Canada* (Ottawa, Approvisionnements et Services Canada, 1994), préparé par Industrie Canada, et proposera des solutions. Il examinera comment une infrastructure complexe d'information améliorera la croissance et la compétitivité des entreprises canadiennes; comment assurer à tous les Canadiens un accès universel et abordable aux services essentiels; comment établir un équilibre approprié entre la concurrence et la réglementation; comment promouvoir le développement ainsi que la diffusion de la culture et du contenu canadiens.

Le Comité a établi cinq groupes d'étude qui se penchent sur les grands domaines d'intérêt suivants : accès et incidences sociales; culture et contenu canadiens; compétitivité et création d'emplois; apprentissage et formation; recherche-développement : applications et développement du marché. Les groupes d'étude et le Comité se réunissent régulièrement et sont engagés dans diverses activités pour étudier les sujets en question, consulter le public et formuler des recommandations à l'intention du gouvernement fédéral.

Pour évaluer l'intérêt public et accroître la sensibilisation aux questions touchant la protection de la vie privée, Industrie Canada, en collaboration avec le Comité consultatif, a préparé ce document de travail intitulé *La protection de la vie privée et l'autoroute canadienne de l'information.* Industrie Canada publiera d'autres documents de travail sur des questions sociales, économiques et technologiques. Les personnes et les groupes intéressés sont invités à nous faire parvenir par écrit des présentations ou des observations sur les solutions proposées ou sur tout autre aspect du document de travail.

Les présentations doivent être adressées à :

Parke Davis, directeur général
Secrétariat du Comité consultatif
sur l'autoroute de l'information
Bureau 640
Tour Journal Nord
300, rue Slater
OTTAWA (Ont.)
K1A 0C8

Toutes les présentations doivent être reçues au plus tard le 23 décembre 1994 (se référer à la *Gazette du Canada,* Partie I).

Table des matières

La protection de la vie privée et l'autoroute canadienne de l'information ainsi que d'autres documents publiés par Industrie Canada sont disponibles sur le réseau informatique Internet en tapant council@istc.ca.

Les utilisateurs d'un protocole de transfert de fichier, de « Gopher » ou du réseau mondial (World Wide Web) peuvent avoir accès à ces ouvrages, en se servant des adresses suivantes d'Internet :

Protocole de transfert de fichier
debra.dgbt.doc.ca/pub/isc

Gopher
debra.dgbt.doc.ca port 70/Industry Canada Documents

Réseau mondial
http:/debra.dgbt.doc.ca/isc/isc.html

Pour obtenir des imprimés de ce document de travail, s'adresser à :

Service de distribution
Direction générale des communications
Industrie Canada
Bureau 208D, Tour est
235, rue Queen
OTTAWA (Ont.)
K1A 0H5
Téléphone : (613) 954-5716
Télécopieur : (613) 954-6436

Une publication complémentaire, *L'autoroute canadienne de l'information : Une nouvelle infrastructure de l'information et des communications au Canada,* est aussi disponible auprès de ce service.

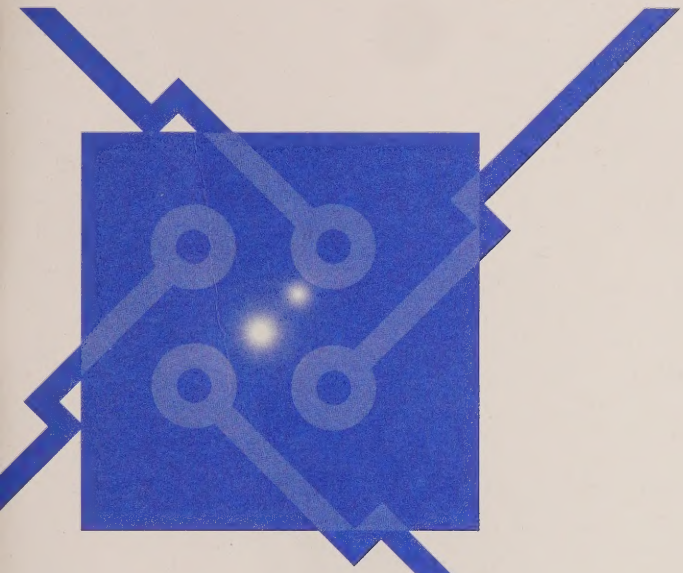
Pour obtenir des renseignements sur le contenu de ce document de travail et sur le processus de consultation, s'adresser à :

Secrétariat du Comité consultatif
sur l'autoroute de l'information
Bureau 640
Tour Journal Nord
300, rue Slater
OTTAWA (Ont.)
K1A 0C8
Téléphone : (613) 990-4268
Télécopieur : (613) 941-1164.

N° au cat. C2-229/1-1994
ISBN 0-662-61370-8
SIT PU 0025-94-03

La protection de la vie privée et l'autoroute canadienne de l'information

Direction générale du développement des communications
et de la planification
Secteur du spectre, des technologies de l'information
et des télécommunications
Industrie Canada
Octobre 1994



La protection de la vie privée et l'autoroute canadienne de l'information

Une nouvelle infrastructure de l'information et des communications au Canada

Industrie Canada Industry Canada

Canada